UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF WISCONSIN

RICHARD DUSTERHOFT, *et al.*, Plaintiffs, v. ONETOUCHPOINT CORP., Defendant.	Case No. 22-cv-0882-bhl **CONSOLIDATED AND AMENDED CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Plaintiffs Sheila Crosby, Richard Dusterhoft, Robin Guertin, Michael Meeks, Michael Meza, Shira Haid, Aria Nardi, Jeffrey Neil Young, and Marcie Strickland ("Plaintiffs"), individually and on behalf of all others similarly situated (collectively, "Class Members"), by and through their attorneys, bring this Consolidated and Amended Class Action Complaint against Defendant OneTouchPoint Corp. ("OTP" or "Defendant") and complain and allege upon personal knowledge as to themselves and upon information and belief as to all other matters.

INTRODUCTION

1. Plaintiffs bring this class action against OTP for its failure to secure and safeguard their and approximately 2.6 million other individuals' personally identifiable information ("PII") and personal health information ("PHI") (collectively, "Private Information").

2. Defendant is a mailing and printing services vendor, which offers print, marketing execution, and supply chain management services to organizations in the healthcare sector.

3. As a condition of receiving services, OTP's clients and their patients are required to provide and entrust OTP with sensitive and private information, including PII and PHI. The PII and PHI that OTP collects and maintains includes names, addresses, healthcare member IDs, and other medical information provided or obtained during health assessments.

4. On or around April 28, 2022, OTP detected encrypted files on some of its systems and began investigating the incident.

5. OTP's investigation later revealed that an unauthorized party had accessed certain OTP servers on April 27, 2022 (the "Data Breach").

6. On or around June 3, 2022, OTP provided a summary of its investigation to its customers. For the most part, it did not send out letters to individuals impacted by the breach until July 27, 2022. In some cases, it did not send out letters to impacted individuals at all.

7. OTP's original notice letter provided scant detail, particularly considering the size and scope of the Data Breach and the sensitivity of Plaintiffs' and Class Members' compromised information. OTP's notice states, in relevant part, that "OTP discovered encrypted files on certain computer systems" which led them to "launch[] an investigation…to determine the nature and scope of the activity," and that OTP's "investigation determined that there was unauthorized access on certain OTP servers beginning on April 27, 2022." OTP also stated that it "later determined that the impacted systems contained information related to individuals provided by our customers," but that it was "unable to say definitively what personal information was accessed by the unauthorized actor" and that "the specific data elements vary for each potentially affected individual."

8. OTP's notice did not disclose how long cybercriminals had access to its systems, how it discovered the encrypted files on its computer systems, the means and mechanism of the cyberattack, the reason for the month-and-a-half delay in notifying Plaintiffs and the Class of the Data Breach, how OTP determined that the Private Information had been "viewed" by the unauthorized actor, and, importantly, what steps OTP took following the Data Breach to secure its systems and prevent future cyberattacks.

9. OTP further did not initially disclose the full extent of the Data Breach. In July, OTP originally reported that the breach had impacted 1,073,316 individuals. However, on or around September 7, 2022, OTP provided an updated breach notice to the Maine Attorney General's office stating that the Data Breach actually impacted more than 2.6 million individuals.

10. OTP reported that the scope of information involved includes an individual's name, member ID, and information that may have been provided during a health assessment, including dates of service, description of service, diagnosis codes, medication, medical recommendations, and other medical information.

11. The Data Breach was a direct result of OTP's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect patients' and employees' PII and PHI from the foreseeable thread of a cyberattack.

12. By taking possession and control of Plaintiffs' and Class Members' Private Information for its own pecuniary benefit, OTP assumed a duty to Plaintiffs and Class Members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard Plaintiffs' and Class Members' Private Information against unauthorized access and disclosure. OTP also had a duty to adequately safeguard this Private Information under industry standards and duties imposed by statutes, including HIPAA regulations and Section 5 of the Federal Trade Commission Act ("FTC Act"). OTP breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect patients' Private Information from unauthorized access and disclosure.

13. As a result of OTP's inadequate security and breach of its duties and obligations, the Data Breach occurred, Plaintiffs and over two and a half million Class Members suffered injury and ascertainable losses in the form of out-of-pocket expenses, loss of value of their time

reasonably incurred to remedy or mitigate the effects of the attack, the diminution in value of their personal information from its exposure, and the present and imminent thread of fraud and identity theft, among other things. This action seeks to remedy these failings and their consequences.

14. The injury to Plaintiffs and Class Members was compounded by the fact that OTP did not notify patients that their Private Information was subject to unauthorized access and exfiltration until July 27, nearly three months after the Data Breach was discovered, and did not reveal the full scope of the Data Breach—which impacted twice as many individuals as OTP originally reported—until on or around September 1, 2022. OTP's failure to timely notify the victims of its Data Breach meant that Plaintiffs and Class Members were unable to take affirmative measures to prevent or mitigate the resulting harm. In some cases, it did not notify patients at all.

15. Despite having been accessed and exfiltrated by unauthorized criminal actors, Plaintiffs' and Class Members' sensitive and confidential Private Information still remains in the possession of OTP. Absent additional safeguards and independent review and oversight, the information remains vulnerable to further cyberattacks and theft.

16. OTP disregarded the rights of Plaintiffs and Class Members by, *inter alia*, failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard patient PII; failing to take standard and reasonably available steps to prevent the Data Breach; failing to properly train its staff and employees on proper security measures; and failing to provide Plaintiffs and Class Members prompt and adequate notice of the Data Breach.

17. In addition, OTP and its employees failed to properly monitor the computer network and systems that housed the Private Information. Had OTP properly monitored these electronic systems, it would have discovered the intrusion sooner or prevented it altogether.

18. The security of Plaintiffs' and Class Members' identities is now at risk because of OTP's wrongful conduct as the Private Information that OTP collected and maintained is now in the hands of data thieves. This present risk will continue for the course of their lives.

19. Armed with the Private Information accessed in the Data Breach, data thieves can commit a wide range of crimes including, for example, opening new financial accounts in Class Members' names, taking out loans in their names, using Class Members' identities to obtain government benefits, filing fraudulent tax returns using their information, obtaining driver's licenses in Class Members' names, obtaining medical services, insurance coverage and medications, and giving false information to police during an arrest.

20. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a present and imminent risk of fraud and identity theft. Among other measures, Plaintiffs and Class Members must now and in the future closely monitor their financial accounts and medical records to guard against identity theft. Further, Plaintiffs and Class Members will incur out-of-pocket costs to purchase credit monitoring and identity theft protection and insurance services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

21. Plaintiffs and Class Members will also be forced to expend additional time to review credit reports and monitor their financial accounts and medical records for fraud or identity theft. Due to the fact that the exposed information potentially includes Social Security numbers ("SSNs") and other immutable personal details, Plaintiffs and Class Members will be at risk of identity theft and fraud that will persist throughout the rest of their lives.

22. Plaintiffs bring this action on behalf of themselves and individuals in the United States whose Private Information was exposed as a result of the Data Breach, which OTP learned of on or about April 28, 2022, and first publicly acknowledged on or about July 27, 2022. Plaintiffs and Class Members seek to hold OTP responsible for the harms resulting from the massive and preventable disclosure of such sensitive and personal information. Plaintiffs seek to remedy the harms resulting from the Data Breach on behalf of themselves and all similarly situated individuals whose Private Information was accessed and exfiltrated during the Data Breach.

23. Plaintiffs and Class Members thus seek actual damages, statutory damages, restitution, injunctive and declaratory relief (including significant improvements to OTP's data security protocols and employee training practices), reasonable attorneys' fees, costs, expenses incurred in bringing this action, and all other remedies this Court deems just and proper.

PARTIES

Plaintiffs

24. Plaintiff Michael Meza is a resident and citizen of the State of Arizona.

25. Plaintiff Michael Meeks is a resident and citizen of the State of Georgia.

26. Plaintiff Marcie Strickland is a resident and citizen of the State of Georgia.

27. Plaintiff Jeffrey Neil Young is a resident and citizen of the State of Maine.

28. Plaintiff Richard Dusterhoft is a resident and citizen of the State of Minnesota.

29. Plaintiff Robin Guertin is a resident and citizen of the State of South Carolina.

30. Plaintiff Shira Haid is a resident and citizen of the State of Wisconsin.

31. Plaintiff Aria Nardi is a resident and citizen of the State of Wisconsin.

32. Plaintiff Sheila Crosby is a resident and citizen of the State of Wisconsin.

Defendant

33. Defendant OneTouchPoint Corp. is a Delaware corporation with its principal place of business located at 1225 Walnut Ridge Dr., Hartland, Wisconsin 53029.

JURISDICTION AND VENUE

34. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because at least one member of the Class is a citizen of a different state than Defendant, there are more than 100 Members of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interests and costs.

35. This Court has personal jurisdiction over OTP because OTP maintains its principal place of business in Wisconsin and conducts substantial business in Wisconsin and in this district through its principal place of business; engaged in the conduct at issue herein from and within this District; and otherwise has substantial contacts with this District and purposely availed itself of the Courts in this District.

36. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(1) and (2) because OTP resides in this district, and this district is where a substantial part of the acts, omissions, and events giving rise to Plaintiffs' claims occurred.

FACTUAL ALLEGATIONS

A. Overview of OTP

37. OTP is a software and business services company incorporated in Delaware with its principal place of business in Hartland, Wisconsin. OTP provides online and offline traditional marketing and communication strategies to healthcare providers. The company provides a range of services to its corporate clients, including brand management, local marketing, marketing execution, print production, and supply chain logistics.

38. In the regular course of its business, OTP collects and maintains the Private Information of patients, former patients, and other persons through its healthcare provider customers to whom it is currently providing or previously provided health-related or other services.

39. As a regular part of its business, OTP requires patients to provide personal information to its healthcare customers before it provides them services. That information includes, *inter alia*, names, addresses, dates of birth, health insurance information, healthcare information, and/or Social Security numbers. OTP stores this information digitally.

40. As a HIPAA covered business entity (*see infra*), OTP is required to implement adequate safeguards to prevent unauthorized use or disclosure of Personal Information, including by implementing requirements of the HIPAA Security Rule[1] and to report any unauthorized use or disclosure of Personal Information, including incidents that constitute breaches of unsecured protected health information as in the case of the Data Breach complained of herein.

41. OTP's Privacy Policy states that it has "put in place appropriate procedures with the service providers we share your Personally Identifiable Information with to ensure that your Personally Identifiable Information is treated by those service providers in a way that is consistent with, and which respects the applicable laws on data security and privacy."[2]

42. However, OTP did not maintain adequate security to protect its systems from infiltration by cybercriminals, and it waited nearly three months to disclose the Data Breach publicly.

[1] The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. *See* 45 C.F.R. Part 160 and Part 164, Subparts A and C.

[2] *See* OTP Privacy Policy, https://1touchpoint.com/privacy-policy.

43. Plaintiffs and the Class Members are, or were, patients of OTP's healthcare provider customers and entrusted OTP with their Private Information.

B. OTP is a HIPAA covered business associate

44. OTP is a HIPAA covered business associate that provides services to various health care providers (i.e., HIPAA "Covered Entities"). As a regular and necessary part of its business, OTP collects and custodies the highly sensitive PII of its clients' patients and health plan Members. OTP is required under federal and state law to maintain the strictest confidentiality of the patient's and plan Members' Private Information that it requires, receives, and collects, and OTP is further required to maintain sufficient safeguards to protect that Private Information from being accessed by unauthorized third parties.

45. As a HIPAA covered business entity, OTP is required to enter into contracts with its Covered Entities to ensure that it will implement adequate safeguards to prevent unauthorized use or disclosure of Private Information, including by implementing requirements of the HIPAA Security Rule[3] and to report to the Covered Entities any unauthorized use or disclosure of Private Information, including incidents that constitute breaches of unsecured protected health information as in the case of the Data Breach complained of herein.

46. As a condition of receiving OTP's services, OTP requires that Covered Entities and their patients and plan Members, including Plaintiffs and Class Members, entrust it with highly sensitive personal information. Due to the nature of OTP's business, which includes providing brand management, local marketing, marketing execution, print production and supply chain logistics, OTP would be unable to engage in its regular business activities without collecting

[3] The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. *See* 45 C.F.R. Part 160 and Part 164, Subparts A and C.

and aggregating Private Information that it knows and understands to be sensitive and confidential.

47. OTP advertises its services as allowing healthcare provider customers to serve "more patients, [with] fewer risks." It promotes the ability for a healthcare provider customer to manage its brand "across departments, clinic locations and hospital affiliates, create and execute prescriptive marketing campaigns and enable offline and online marketing efforts at the local level – all while ensuring [a customer's] messaging and assets are compliant in this highly regulated industry."[4]

48. OTP's website touts security as a main feature of its software, stating that its software is "designed around compliance" and it "ensure[s] compliance with state and federal regulations" and that OTP allows customers to "execute HIPAA compliant patient communications." OTP stresses that it adheres "to the strictest HIPAA standards and ensure[s] that the handling of protected health information (PHI) is secure." To this end, it "will sign a Business Associates Agreement (BAA) with [its] customers to become joint custodians of protected health information (PHI)."[5]

49. OTP further emphasizes on its website that it has "compliance expertise" and is "part of an exclusive group of organizations worldwide certified as HITRUST," explaining that its "security framework ensures that [its] solutions are built within secure web-based technology and allow[s] member communications to be published to print, web, and email." It touts the following as supporting its compliance expertise: "HIPPA compliant;" "PHI, PII, PCI, SSN, and

[4] *Healthcare*, ONETOUCHPOINT, https://1touchpoint.com/solutions/healthcare (last visited Nov. 14, 2022).
[5] *Id.*

critical system data;" "[u]ser access controls;" "[e]nd-to-end email encryption;" and "[s]ecure web interface with single sign-on."[6]

50. OTP's Privacy Policy on its website states that OTP maintains "commercially reasonable security measures to protect the Personally Identifiable Information [it] collect[s] and store[s] from loss, misuse, destruction, or unauthorized access."[7]

51. Plaintiffs and Class Members are or were patients whose medical records were maintained by, or who received health-related or other services from, OTP through its healthcare provider customers, and directly or indirectly entrusted OTP with their Private Information. Plaintiff and Class Members reasonably expected that OTP would safeguard their highly sensitive information and keep their Private Information confidential.

C. The Data Breach Compromised Plaintiffs' and Class Members' Private Information

52. On or about April 28, 2022, according to the notice OTP provided to Plaintiffs[8] and Class Members, OTP discovered encrypted files on certain computer systems. It launched an investigation with the assistance of third-party forensic specialists to determine the nature and scope of the activity.

53. OTP's investigation determined that there was unauthorized access to certain OTP servers beginning on April 27, 2022.

54. OTP did not publicly announce the Data Breach until three months later. It provided a summary of its investigation to its healthcare provider customers beginning on June 3, 2022. It worked with its customers to determine what Private Information was stored on the

---

[6] *Healthcare Insurance Member Communications*, ONETOUCHPOINT, https://1touchpoint.com/solutions/health-insurance (last visited Nov. 14, 2022).

[7] *Privacy Policy*, ONETOUCHPOINT, https://1touchpoint.com/privacy-policy (last visited Nov. 14, 2022).

[8] In some cases, Plaintiffs were provided with notice from their healthcare provider—not OTP.

OTP network and to whom that information related. On or around July 27, 2022, OTP began to notify patients via letter about the data breach that occurred in April 2022. The press release OTP posted on its website states: "[T]he scope of information potentially involved includes an individual's name, member ID, and information that may have provided during a health assessment."[9]

55. OTP's notice letter also vaguely describes the measures it took following its discovery of the Data Breach, stating only that:

> Upon discovery, we immediately commenced an investigation to confirm the nature and scope of the incident. We reported this incident to law enforcement, and we are taking steps to implement additional safeguards and review policies and procedures relating to data privacy and security.

56. OTP's notice omits pertinent information including how long criminals gained access to the encrypted files on its systems, what computer systems were impacted, the means and mechanisms of the cyberattack, the reason for the one and a half month delay in notifying Plaintiffs and Class Members of the Data Breach, how it determined that the Private Information had been "viewed" or "accessed," and of particular importance to Plaintiffs and Class Members, what actual steps OTP took following the Data Breach to secure its systems and prevent further cyberattacks.

57. Based on OTP's acknowledgment that personal information was "accessed by the unauthorized actor," it is evident that unauthorized criminal actors did in fact access OTP's network and exfiltrate Plaintiffs' and Class Members' Private Information in an attack designed to acquire that sensitive, confidential, and valuable information.

58. The Private Information contained in the files accessed by cybercriminals appears not to have been encrypted because if properly encrypted, the attackers would have acquired

[9] *Notice of Data Security Incident*, ONETOUCHPOINT, https://1touchpoint.com/notice-of-data-event (last visited Nov. 14, 2022).

unintelligible data and would not have "accessed" Plaintiffs and Class Members Private Information.

59. OTP said it later determined that the compromised systems contained Private Information provided by its customers, including names, addresses, birth dates, date of service, descriptions of services, diagnoses codes, information provided as part of a health assessment, and member IDs. Customers have reported the Data Breach as involving names, subscriber ID numbers, diagnoses, medications, addresses, dates of birth, sexes, physicians, demographic information, family histories, social histories, allergies, vitals, immunizations, and other information. For at least one covered entity, the hacked information also contained Social Security numbers. [10]

60. OTP initially identified 34 healthcare insurance companies and healthcare services providers involved in the data breach, though recent reports indicate that number is closer to 40, which is potentially subject to increase as new details emerge.[11] Common Ground Healthcare Cooperative and Medical Mutual of Ohio each submitted reports regarding the OTP Data Breach to the Health and Human Services Office for Civil Rights recently. Common Ground Healthcare confirmed that 133,714 of its Members were affected.[12]

---

[11] *See 30 Healthcare providers impacted after OneTouchPoint data breach*, SECUREBLINK (Jul. 30, 2022), https://www.secureblink.com/cyber-security-news/30-healthcare-providers-impacted-after-one-touch-point-data-breach (last visited Aug. 16, 2022) (indicating that at least two more businesses have submitted notices of being impacted by the Data Breach that were not included among those listed on OneTouch's website); Steven, *OneTouchPoint's Data Breach*, Strong (Sept. 2, 2022), available: https://www.idstrong.com/sentinel/onetouchpoints-data-breach/ (last visited Nov. 14, 2022) (indicated that the current total of impacted health plans is 40, but that "the figure can potentially expand in the future as more details are revealed").

[12] *OneTouchPoint Ransomware Victim Count Increases to 2.65 Million*, HIPAA JOURNAL (Sept. 1, 2022), available: https://www.hipaajournal.com/onetouchpoint-ransomware-victim-count-increases-to-2-65-million/ (last accessed Nov. 14, 2022).

61. In July, OTP originally reported that the Data Breach impacted 1,073,316 individuals. However, on or around September 1, 2022, OTP provided an updated breach notice to the Maine Attorney General's office stating that the breach actually impacted 2,651,396 individuals.[13]

62. As a HIPAA associated business entity that collects, creates, and maintains significant volumes of Private Information, the targeted attack was a foreseeable risk of which OTP was aware and knew it had a duty to guard against.

63. The targeted attack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Private Information of patients and/or plan Members, like Plaintiffs and Class Members.

64. Despite detecting the Data Breach on or around April 27, 2022, OTP waited more than a month following the completion of its investigation to notify the impacted individuals of the Data Breach and of the need for them to protect themselves against fraud and identity theft. OTP was, of course, too late in the discovery and notification of the Data Breach.

65. Due to OTP's inadequate security measures and its delayed notice to victims, Plaintiffs and Class Members now face a present, immediate, and ongoing risk of fraud and identity theft that they will have to deal with for the rest of their lives.

66. OTP had obligations created by HIPAA, contract, industry standards and common law made to Plaintiffs and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

67. Plaintiffs and Class Members entrusted their Private Information to OTP's clients with the reasonable expectation and mutual understanding that OTP or anyone who used their

[13] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/d90babd7-ded0-457b-8a6e-66360be5c9cc.shtml (last visited Nov. 14, 2022).

Private Information in conjunction with the healthcare services they received would comply with obligations to keep such information confidential and secure from unauthorized access after it received such information.

68. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, OTP assumed legal and equitable duties and knew, or should have known, that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

69. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their personal information. Plaintiffs and Class Members would not have allowed OTP or anyone in OTP's position to receive their Private Information had they known that OTP would fail to implement industry standard protections for that sensitive information.

70. As a result of OTP's negligent and wrongful conduct, Plaintiffs' and Class Members' highly confidential and sensitive Private Information was left exposed to cybercriminals.

D. Defendant Was Obligated Under HIPAA to Safeguard the Private Information

71. OTP is a covered business associate under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

72. OTP is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[14] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

73. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

74. HIPAA's Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

75. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

76. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

77. HIPAA's Security Rule requires OTP to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

[14] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

d. Ensure compliance by its workforce.

78. HIPAA also requires OTP to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, OTP is required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

79. HIPAA and HITECH also obligated OTP to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

80. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires OTP to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."[15]

81. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

82. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

[15] Breach Notification Rule, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (last visited Nov. 14, 2022) (emphasis added).

83. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." US Department of Health & Human Services, Security Rule Guidance Material.[16] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says, "represent the industry standard for good business practices with respect to standards for securing e-PHI." US Department of Health & Human Services, Guidance on Risk Analysis.[17]

E. OTP Failed to Follow FTC Guidelines

84. OTP was also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

85. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices.

[16] http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html (last visited Nov. 14, 2022).

[17] https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html (last visited Nov. 14, 2022).

86. According to the FTC, the need for data security should be factored into all business decision-making.

87. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses.

88. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

89. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

90. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

91. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

92. OTP failed to properly implement basic data security practices.

93. OTP's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' and plan Members Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

94. OTP was at all times fully aware of its obligation to protect the Private Information of the patients and plan Members whose Private Information it stored. OTP was also aware of the significant repercussions that would result from its failure to do so.

F. OTP Failed to Comply with Industry Standards

95. As described above, experts studying cybersecurity routinely identify healthcare providers and their business associates as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

96. Several best practices have been identified that at a minimum should be implemented by HIPAA covered business entities like OTP, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

97. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; protecting against any possible communication system; and training staff regarding critical points.

98. OTP failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3,

DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

99. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and OTP failed to comply with these accepted standards, thereby opening the door to cybercriminals and causing the Data Breach.

G. OTP Owed Plaintiffs and Class Members a Duty to Safeguard Their Private Information

100. In addition to its obligations under federal and state laws, OTP owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. OTP owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Class Members.

101. OTP owed a duty to Plaintiffs and Class Members to create and implement reasonable data security practices and procedures to protect the Private Information in its possession, including adequately training its employees and others who accessed Private Information within its computer systems on how to adequately protect Private Information.

102. OTP owed a duty to Plaintiffs and Class Members to implement processes that would detect a compromise of Private Information in a timely manner.

103. OTP owed a duty to Plaintiffs and Class Members to act upon data security warnings and alerts in a timely fashion.

104. OTP owed a duty to Plaintiffs and Class Members to disclose in a timely and accurate manner when and how the Data Breach occurred.

105. OTP owed a duty of care to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

106. OTP owes a legal duty to secure consumers' PII and PHI and to timely notify consumers of a data breach. The Wisconsin Constitution contains a Right to Privacy clause to protect PII, such as the data exposed through the Data Breach.

107. Moreover, Wisconsin has codified the right to privacy in its codification of traditional common law torts in Wis. Stat. § 995.50(2). Wisconsin's Right to Privacy statute provides: "The right of privacy is recognized in this state." Moreover, the Right to Privacy statute states that an invasion of privacy occurs when "the privacy of another" is intruded upon in a "nature highly offensive to a reasonable person, in a place that a reasonable person would consider private or in a manner which is actionable for trespass." Wis. Stat. § 995.50(2)(a).

108. OTP's failure to implement reasonable measures to secure consumers' PII and PHI violates Wis. Stat. § 995.50(2). Despite OTP's commitment to protecting personal information and its legal requirements to do so under Federal and Wisconsin law, OTP failed to prioritize data and cyber security by adopting reasonable data- and cyber-security measures to prevent and detect the unauthorized access to Plaintiff's and Class Members' PII and PHI.

109. Had OTP remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, OTP could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiffs' and Class Members' confidential PII.

H. OTP Knew that Criminals Target Private Information

110. OTP's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry and other industries holding significant amounts of PII and PHI preceding the date of the breach.

111. At all relevant times, OTP knew, or should have known, its patients', Plaintiffs', and all other Class Members' Private Information was a target for malicious actors. Despite such knowledge, OTP failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiffs' and Class Members' Private Information from cyber-attacks that OTP should have anticipated and guarded against.

112. The targeted attack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Private Information of patients and/or plan Members, like Plaintiffs and Class Members.

113. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2022 report, the healthcare compliance company Protenus found that there were 905 medical data breaches in 2021, leaving over 50 million patient records exposed for 700 of the 2021 incidents. This is an increase from the 758 medical data breaches that Protenus compiled in 2020.[18]

114. The healthcare sector suffered about 337 breaches in the first half of 2022 alone, according to Fortified Health Security's mid-year report released in July. The percentage of

[18] *2022 Breach Barometer*, PROTENUS, https://www.protenus.com/breach-barometer-report (last visited Nov. 14, 2022).

healthcare breaches attributed to malicious activity rose more than 5 percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.[19]

115. Further, a 2022 report released by IBM Security states that for 12 consecutive years the healthcare industry has had the highest average cost of a data breach and as of 2022 healthcare data breach costs have hit a new record high.[20]

116. Private Information is a valuable property right.[21] The value of Private Information as a commodity is measurable.[22] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[23] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[24] Private Information is so valuable to identity thieves that once Private Information has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

---

[19] Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, Cybersecurity News (July 19, 2022), available: https://healthitsecurity.com/news/health-sector-suffered-337-healthcare-data-breaches-in-first-half-of-year (last visited October 5, 2022).

[20] *Cost of a Data Breach Report 2022*, IBM Security, available: https://www.ibm.com/downloads/cas/3R8N1DZJ (last visited Nov. 14, 2022).

[21] *See* Marc van Lieshout, *The Value of Personal Data*, 457 IFIP ADVANCES IN INFORMATION AND COMMUNICATION TECHNOLOGY 26 (May 2015), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible...") (last visited Nov. 14, 2022).

[22] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE (Apr. 28, 2014), http://www.medscape.com/viewarticle/824192 (last visited Nov. 14, 2022).

[23] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD 4 (Apr. 2, 2013), Exploring the Economics of Personal Data : A Survey of Methodologies for Measuring Monetary Value | OECD Digital Economy Papers | OECD iLibrary (oecd-ilibrary.org) (last visited Nov. 14, 2022).

[24] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/ (last visited Nov. 14, 2022).

117. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, SSNs, Private Information, and other sensitive information directly on various Internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

118. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[25] A cybercriminal who steals a person's PHI can end up with as many as "seven to 10 personal identifying characteristics of an individual."[26] A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[27]

119. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[28] According to a report released by the Federal Bureau of Investigation's

[25] *See* Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH MAGAZINE (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.") (last visited Nov. 14, 2022).

[26] *Id.*

[27] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010, 5:00 AM), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims (last visited Nov. 14, 2022).

[28] Adam Greenberg, *Health insurance credentials fetch high prices in the online black market*, SC MAGAZINE (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market (last visited Nov. 14, 2022).

("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[29]

120. Criminals can use stolen Private Information to extort a financial payment by "leveraging details specific to a disease or terminal illness."[30] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion…By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[31]

121. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[32]

122. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' Private Information has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

123. Indeed, cyberattacks against the healthcare industry have been common for over ten years with the Federal Bureau of Investigation ("FBI") warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system

[29] *See Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI CYBER DIVISION (Apr. 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf (last visited Nov. 14, 2022).

[30] *See* n.8, *supra*.

[31] *Id.*

[32] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior*, *An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011), https://www.jstor.org/stable/23015560?seq=1 (last visited Nov. 14, 2022).

is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[33]

124. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals… because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[34]

125. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[35]

126. OTP was on notice that the FBI has recently been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[36]

---

[33] Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector (Nov. 14, 2022).

[34] *FBI, Secret Service Warn of Targeted Ransomware*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited Nov. 14, 2021).

[35] *See* Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack, Security Magazine* (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last visited Nov. 14, 2022).

[36] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820 (last visited Nov. 14, 2022).

127. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[37]

128. As implied by the above AMA quote, stolen Private Information can be used to interrupt important medical services. This is an imminent and certainly impending risk for Plaintiffs and Class Members.

129. OTP was on notice that the federal government has been concerned about healthcare company data encryption practices. OTP knew its employees accessed and utilized protected health information in the regular course of their duties, yet it appears that information was not encrypted.

130. The OCR urges the use of encryption of data containing sensitive personal information. As far back as 2014, the Department fined two healthcare companies approximately two million dollars for failing to encrypt laptops containing sensitive personal information. In announcing the fines, Susan McAndrew, formerly OCR's deputy director of health information privacy, stated in 2014 that "[o]ur message to these organizations is simple: encryption is your best defense against these incidents."[38]

---

[37] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED. ASS'N (Oct. 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (last visited Nov. 14, 2022).

[38] "Stolen Laptops Lead to Important HIPAA Settlements," U.S. Dep't of Health and Human Services (Apr. 22, 2014), available at https://wayback.archive-it.org/3926/20170127085330/https://www.hhs.gov/about/news/2014/04/22/stolen-laptops-lead-to-important-hipaa-settlements.html (Nov. 14, 2022).

131. As a HIPAA covered business associate, OTP should have known about its data security vulnerabilities and implemented enhanced and adequate protection, particularly given the nature of the Private Information stored in its unprotected files.

I. Theft of Private Information Has Grave and Lasting Consequences for Victims

132. Theft of Private Information is serious. The FTC warns consumers that identity thieves use Private Information to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[39]

133. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[40] According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan, change a billing address so the victim no longer receives bills, open new utilities, obtain a mobile phone, open a bank account and write bad checks, use a debit card number to withdraw funds, obtain a new driver's license or ID, and/or use the victim's information in the event of arrest or court action.[41]

134. With access to an individual's Private Information, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a

---

[39] *See What to Know About Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER ADVICE, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last visited Nov. 14, 2022).

[40] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 12 C.F.R. § 1022.3(g).

[41] Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself?*, EXPERIAN (Sept. 1, 2017), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/ (last visited Nov. 14, 2022).

driver's license or official identification card in the victim's name but with the thief's picture, using the victim's name and SSN to obtain government benefits, or filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[42]

135. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States. For example, with the Private Information stolen in the Data Breach, which includes Social Security numbers, identity thieves can open financial accounts, commit medical fraud, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft. These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and Class Members.

136. Private Information is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it and trade the information on dark web, black-markets for years.

137. For example, it is believed that certain highly sensitive personal information compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related unemployment benefits.

138. The Private Information exposed in this Data Breach is valuable to identity thieves for use in the kinds of criminal activity described herein. These risks are both certainly impending

[42] *See Warning Signs of Identity Theft*, FEDERAL TRADE COMMISSION, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited Nov. 14, 2022).

and substantial. As the FTC has reported, if cyber thieves get access to a person's highly sensitive information, they will use it.[43]

139. Cyber criminals may not use the information right away. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[44]

140. Social security numbers are particularly sensitive pieces of personal information. As the Consumer Federation of America explains:

> **Social Security number:** *This is the most dangerous type of personal information in the hands of identity thieves* because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refund, employment—even using your identity in bankruptcy and other legal matters. It's hard to change your Social Security number and it's not a good idea because it is connected to your lift in so many ways. [45]

141. For instance, with a stolen Social Security number, which is only one subset of the Private Information compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[46]

142. Identity thieves can use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the

---

[43] Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017), https://www.militaryconsumer.gov/blog/how-fast-will-identity-thieves-use-stolen-info (last visited Nov. 14, 2022).

[44] *Data Breaches Are Frequent*, *supra* note 11.

[45] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 15, 2017, https://www.usatoday.com/story/money/personalfinance/2017/11/15/5-ways-identity-thief-can-use-your-social-security-number/860643001/ (last visited Nov. 14, 2022) (emphasis added).

[46] *Id.*

victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

143. This was a financially motivated Data Breach, as the only reason the cybercriminals go through the trouble of running a targeted cyberattack against companies like OTP is to get information that they can monetize by selling on the black market for use in the kinds of criminal activity described herein. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."

144. Indeed, a social security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[47] "[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web."[48]

145. The medical information, PHI, which was exposed is also highly valuable. PHI can sell for as much as $363 according to the Infosec Institute.[49]

[47] Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web*, Nov. 15, 2017, https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web (last visited Nov. 14, 2022).

[48] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/ (last visited Nov. 14, 2022).

[49] Center for Internet Security, *Data Breaches: In the Healthcare Sector, available at:* https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/ (last visited Nov. 14, 2022).

146. These risks are both certainly impending and substantial. As the FTC has reported, if hackers get access to PII, they *will use it.*[50]

147. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[51]

148. Theft of SSNs also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of her SSN, and a new SSN will not be provided until after the victim has suffered the harm.

149. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you haven't gotten a credit freeze yet, you're easy pickings."[52]

150. Theft of PII is even more serious when it includes theft of PHI. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

---

[50] *Id.*

[51] *2021 Consumer Aftermath Report: How Identity Crimes Impact Victims, their Families, Friends, and Workplaces*, IDENTITY THEFT RESOURCE CENTER (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/ (last visited Nov. 14, 2022).

[52] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (Aug. 5, 2019, 3:39 PM), https://time.com/5643643/capital-one-equifax-data-breach-social-security/ (last visited Nov. 14, 2022).

151. Medical identity theft is one of the most common, most expensive, and most difficult-to-prevent forms of identity theft. Medical identify theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. According to Kaiser Health News, "medical-related identity theft accounted for 43 percent of all identity thefts reported in the United States in 2013," which is more than identity thefts involving banking and finance, the government and the military, or education.[53] "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum.[54] "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[55]

152. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[56] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[57] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use Private Information "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care." [58] The FTC also warns, "If the thief's

[53] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/ (last visited Nov. 14, 2022).

[54] *Id*.

[55] *Id.*

[56] Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, WORLD PRIVACY FORUM 6 (Dec. 12, 2017), https://www.worldprivacyforum.org/2017/12/new-report-the-geography-of-medical-identity-theft/ (last visited Nov. 14, 2022).

[57] *See* n.24, *supra*.

[58] *See* n.35, *supra*.

health information is mixed with yours, it could affect the medical care you're able to get or the health insurance benefits you're able to use. It could also hurt your credit."[59]

153. A report published by the World Privacy Forum and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.
- Significant bills for medical goods and services not sought nor received.
- Issues with insurance, co-pays, and insurance caps.
- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.
- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.
- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.
- Phantom medical debt collection based on medical billing or other identity information.
- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.[60]

154. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. Fraud and identity theft resulting from the Data Breach may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security Number was used to file

[59] *Id.*

[60] *See* n.52, *supra*.

for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

155. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, and it takes some individuals up to three years to learn that information.[61]

156. Further, criminals often trade stolen Private Information on the "cyber black-market" for years following a breach. Cybercriminals can post stolen Private Information on the internet, thereby making such information publicly available.

157. Approximately 21% of victims do not realize their identify has been compromised until more than two years after it has happened. [62] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[63]

158. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.[64]

---

[61] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 JOURNAL OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), https://www.iiisci.org/Journal/PDV/sci/pdfs/IP069LL19.pdf (last visited Nov. 14, 2022).

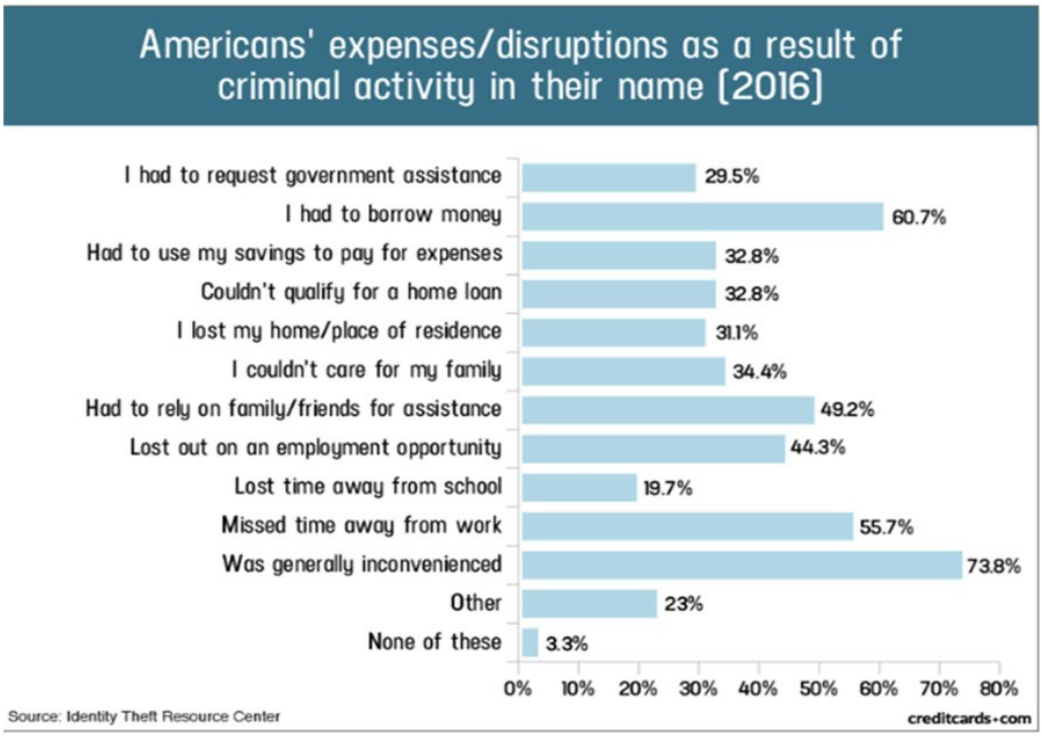
[62] *See* Medical ID Theft Checklist, *available at:* https://www.identityforce.com/blog/medical-id-theft-checklist-2.

[63] Experian, *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches ("Potential Damages*"), *available at:* https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf (last visited Nov. 14, 2022).

[64] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.global-screeningsolutions.com/Guide-for-Assisting-ID-Theft-Victims.pdf (last visited Nov. 14, 2022).

159. It is within this context that Plaintiffs and all other Class Members must now live with the knowledge that their Private Information is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

160. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information.



161. Victims of the Data Breach, like Plaintiffs and Class Members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their privacy and credit because of the Data Breach.[65]

162. As a direct and proximate result of the Data Breach, Plaintiffs and Class Members have had their Private Information exposed, have suffered harm as a result, and have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

[65] *Id.*

Plaintiffs and Class Members must now take the time and effort (and spend the money) to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services every year for the rest of their lives, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions and healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

163. Plaintiffs and Class Members have suffered or will suffer actual harms for which they are entitled to compensation, including but not limited to the following:

a. Actual identity theft, including fraudulent credit inquiries and cards being opened in their names;

b. Trespass, damage to, and theft of their personal property, including Private Information;

c. Improper disclosure of their Private Information;

d. The imminent and certainly impending injury flowing from actual and potential future fraud and identity theft posed by their Private Information being in the hands of criminals and having already been misused;

e. The imminent and certainly impending risk of having their confidential medical information used against them by spam callers to defraud them;

f. Damages flowing from Defendant's untimely (and in some cases, non-existent) and inadequate notification of the Data Breach;

g. Loss of privacy suffered as a result of the Data Breach;

h. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;

i. Ascertainable losses in the form of deprivation of the value of patients' personal information for which there is a well-established and quantifiable national and international market;

j. The loss of use of and access to their credit, accounts, and/or funds;

k. Damage to their credit due to fraudulent use of their Private Information; and

l. Increased cost of borrowing, insurance, deposits, and other items which are adversely affected by a reduced credit score.

164. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which remains in the possession of Defendant, is protected from further public disclosure by the implementation of better employee training and industry standard and statutorily compliant security measures and safeguards. Defendant has shown itself to be wholly incapable of protecting Plaintiffs' and Class Members' Private Information.

165. Plaintiffs and Class Members also have an interest in ensuring that their personal information that was provided to OTP is removed from OTP's unencrypted files.

166. Defendant itself acknowledged the harm caused by the Data Breach because it offered Plaintiffs and Class Members the inadequate 24 months of identity theft repair and monitoring services. This limited identity theft monitoring is, however, inadequate to protect Plaintiff and Class Members from a lifetime of identity theft risk.

167. Defendant further acknowledged, in its letter to Plaintiff and other Class Members, that, in response to the Data Breach, OTP "worked with our experts to try to prevent such an incident from ever happening again."[66]

168. The letter further acknowledged that the Data Breach would cause inconvenience to affected individuals by providing numerous "steps" for Class Members to take in an attempt to mitigate the harm caused by the Data Breach,[67] and that financial harm would likely occur, stating: "We are notifying potentially impacted individuals, including you, so that you may take steps to protect your information…. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors."

169. At OTP's suggestion, Plaintiffs are trying to mitigate the damage that OTP has caused them. Given the kind of Private Information OTP made accessible to hackers, however, Plaintiffs are certain to incur additional damages. Because identity thieves have their Private Information, Plaintiffs and all Class Members will need to have identity theft monitoring protection for the rest of their lives. Some may even need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with a new number.[68] None of this should have happened.

170. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries. For this reason, Defendant knew or should have known about these dangers and strengthened its data

[66] *Id.*

[67] *Id.*

[68] *What happens if I change my Social Security number?*, LEXINGTON LAW (Aug. 10, 202), https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html (last visited Nov. 14, 2022).

security accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

J. The Data Breach Was Foreseeable

171. Data security breaches have dominated the headlines for the last two decades. And it doesn't take an IT industry expert to know it. The general public can tell you the names of some of the biggest cybersecurity breaches: Target,[69] Yahoo,[70] Marriott International,[71] Chipotle, Chili's, Arby's,[72] and others.[73]

172. Companies providing services to the healthcare industry, such as OTP, have been prime targets for cyberattacks. As early as August 2014, the FBI specifically warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[74] Here, as Defendant explained in the letter it sent to Plaintiffs, OTP "process[es]

---

[69] Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZDNET (Feb. 2, 2015), https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/ (last visited Nov. 14, 2022).

[70] Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSOONLINE.COM (Oct. 4, 2017), https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html (last visited Nov. 14, 2022).

[71] Patrick Nohe, *The Marriot Data Breach: Full Autopsy*, THE SSL STORE: HASHEDOUT (Mar. 22, 2019), https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/ (last visited Nov. 14, 2022).

[72] Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle, Others*, CNET (Aug. 1, 2018), https://www.cnet.com/news/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b (last visited Nov. 14, 2022).

[73] *See, e.g.*, Michael Hill and Dan Swinhoe, *The 15 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Nov. 8, 2022)), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html (last visited Nov. 14, 2022).

[74] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 20, 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idINKBN0GK24U20140820 (last visited Nov. 14, 2022).

information for health plans[.]" Based on information obtained by Plaintiffs, OTP processes health information for major insurance companies, including Blue Cross Blue Shield of Michigan and Matrix, among others.

173. OTP should certainly have been aware, and indeed was aware, that it was at risk for a data breach that could expose the Private Information that it collected and maintained.

174. Indeed, OTP's Privacy Policy states the following:

> We maintain commercially reasonable security measures to protect the Personally Identifiable Information we collect and store from loss, misuse, destruction, or unauthorized access. However, no security measure or modality of data transmission over the Internet is 100% secure. Although we strive to use commercially acceptable means to protect your Personally Identifiable Information, we cannot guarantee absolute security.[75]

175. OTP's assurances of maintaining high standards of cybersecurity make it evident that OTP recognized it had a duty to use "commercially acceptable" measures to protect the Private Information that it collected and maintained. Yet, it appears that OTP did not meaningfully or comprehensively use the reasonable measures, including the "commercially acceptable" means it claims to utilize.

176. OTP was clearly aware of the risks it was taking and the harm that could result from inadequate data security.

K. OTP Could Have Prevented the Data Breach

177. Data disclosures and data breaches are preventable.[76] As Lucy Thompson wrote in the Data Breach and Encryption Handbook, "In almost all cases, the data breaches that occurred

[75] *See* https://1touchpoint.com/privacy-policy (last visited October 27, 2022).

[76] Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[77] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised[.]"[78]

178. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures … Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[79]

179. In a Data Breach like this, many failures laid the groundwork for the Breach. The FTC has published guidelines that establish reasonable data security practices for businesses. The FTC guidelines emphasize the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[80] The guidelines establish that businesses should protect the confidential information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommended that businesses utilize an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming

[77] *Id.* at 17.

[78] *Id.* at 28.

[79] *Id.*

[80] FTC, *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_protecting-personal-information.pdf (last visited Nov. 14, 2022).

traffic for activity indicating hacking attempts; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

180. Upon information and belief, OTP failed to maintain many reasonable and necessary industry standards necessary to prevent a data breach, including the FTC's guidelines. Upon information and belief, OTP also failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework, NIST Special Publications 800-53, 53A, or 800-171; the Federal Risk and Authorization Management Program (FEDRAMP); or the Center for Internet Security's Critical Security Controls (CIS CSC), which are well respected authorities in reasonable cybersecurity readiness.

181. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[81]

182. To prevent and detect malware attacks, Defendant could and should have implemented, as recommended by the Federal Bureau of Investigation, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.

[81] *See* How to Protect Your Networks from RANSOMWARE, at 3, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Nov. 14, 2022)

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[82]

183. Further, to prevent and detect malware attacks, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

[82] *Id.* at 3-4.

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net) ….

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[83]

[83] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited Nov. 14, 2022).

184. In addition, to prevent and detect ransomware attacks, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

- **Secure internet-facing assets**
  - Apply latest security updates
  - Use threat and vulnerability management
  - Perform regular audit; remove privileged credentials
- **Thoroughly investigate and remediate alerts**
  - Prioritize and treat commodity malware infections as potential full compromise;
- **Include IT Pros in security discussions**
  - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;
- **Build credential hygiene**
  - Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords
- **Apply principle of least-privilege**
  - Monitor for adversarial activities
  - Hunt for brute force attempts
  - Monitor for cleanup of Event Logs
  - Analyze logon events
- **Harden infrastructure**
  - Use Windows Defender Firewall
  - Enable tamper protection
  - Enable cloud-delivered protection
  - Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[84]

[84] *See* "Human-operated ransomware attacks: A preventable disaster," (Mar. 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Nov. 14, 2022).

185. Given that OTP was storing the Confidential Information of more than 2.6 million individuals, OTP could and should have implemented all of the above measures to prevent and detect ransomware attacks.

186. Specifically, among other failures, OTP had far too much confidential unencrypted information held on its systems. Such Private Information should have been segregated into an encrypted system.[85] Indeed, the United States Department of Health and Human Services' Office for Civil Rights urges the use of encryption of data containing sensitive personal information, stating "[o]ur message to these organizations is simple: encryption is your best defense against these incidents."[86]

187. In sum, this Data Breach could have readily been prevented through the use of industry standard network segmentation and encryption of all confidential information.

188. Plaintiffs and Class Members entrusted their Private Information to OTP as a condition of receiving healthcare related services from OTP's clients. Plaintiffs and Class Members understood and expected that OTP or anyone in OTP's position would safeguard their PII and PHI against cyberattacks, delete or destroy Private Information that OTP was no longer required to maintain, and timely and accurately notify them if their Private Information was compromised.

[85] *See, e.g.,* Adnan Raja, *How to Safeguard Your Business Data with Encryption*, Aug. 14, 2018, https://digitalguardian.com/blog/how-safeguard-your-business-data-encryption (last visited Nov. 14, 2022).

[86] "Stolen Laptops Lead to Important HIPAA Settlements," U.S. Dep't of Health and Human Services (Apr. 22, 2014), https://www.hcinnovationgroup.com/policy-value-based-care/article/13006731/hhs-stolen-laptops-lead-to-important-hipaa-settlements (last visited Nov. 14, 2022).

L. Plaintiffs' and Class Members Damages

189. OTP failed to inform Plaintiffs and Class Members of the Data Breach in time for them to protect themselves from identity theft.

190. OTP stated that it discovered the Data Breach in April 2022. And yet, OTP did not start notifying affected individuals until July 2022—months after it learned of the Data Breach. Even then, OneTouchPoint failed to inform Plaintiff and Class Members exactly what information was exposed in the Data Breach, leaving Plaintiffs and Class Members unsure as to the scope of information that was compromised. In some cases, it never contacted Plaintiffs.

191. During these intervals, the cybercriminals were exploiting the information while OTP was secretly still investigating the Data Breach.

192. If OTP had investigated the Data Breach more diligently and reported it sooner, Plaintiffs and the Class could have taken steps to protect themselves sooner and to mitigate the damages caused by the Data Breach.

193. To date, OTP has done nothing to provide Plaintiffs and Class Members with relief for the damages they have suffered as a result of the Data Breach. OTP did not even offer identity protection and/or credit monitoring services to those affected by the Data Breach; it merely referred Plaintiffs and Class Members to the three major credit reporting bureaus where Class Members could receive one free credit report and/or access a credit freeze. Not only did OTP fail to provide any ongoing credit monitoring or identity protection services, but the information it provided about credit reports and credit freezes does nothing to compensate Class Members for damages incurred and time spent dealing with the Data Breach.

194. Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

195. As a direct and proximate result of OTP's conduct, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiffs and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

196. Plaintiffs and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on the acquired Private Information, as potential fraudsters could use that information to target such schemes more effectively to Plaintiffs and Class Members.

197. Plaintiffs and Class Members have and will also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

198. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring financial and other sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. Contacting financial institutions and closing or modifying financial accounts; and

f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity presently and for years to come.

199. Plaintiffs and Class Members suffered actual injury from having their Private Information compromised as a result of the Data Breach including, but not limited to: (a) damage to and diminution in the value of their Private Information, a form of property that OTP obtained from Plaintiffs and Class Members; (b) violation of their privacy rights; (c) imminent and impending injury arising from the increased risk of identity theft and fraud; and (d) emotional distress.

200. Further, as a result of OTP's conduct, Plaintiffs and Class Members are forced to live with the anxiety that their Private Information may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy with respect to that information.

201. As a direct and proximate result of OTP's actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and are at an increased present, continuing and imminent increased risk of future harm.

202. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of OTP, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online, is properly encrypted, and that access to such data is password protected.

203. Many failures laid the groundwork for the occurrence of the Data Breach, starting with OTP's failure to incur the costs necessary to implement adequate and reasonable cyber security training, procedures and protocols that were necessary to protect Plaintiffs' and Class Members' Private Information.

204. OTP maintained the Private Information in an objectively reckless manner, making the Private Information vulnerable to unauthorized disclosure.

205. OTP knew, or reasonably should have known, of the importance of safeguarding Private Information and of the foreseeable consequences that would result if Plaintiffs' and Class Members' Private Information was stolen, including the significant costs that would be placed on Plaintiffs and Class Members as a result of a breach.

206. The risk of improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to OTP, and thus OTP was on notice that failing to take necessary steps to secure Plaintiffs' and Class Members' Private Information from that risk left the Private Information in a dangerous condition.

207. OTP disregarded the rights of Plaintiffs and Class Members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that the Private Information was protected against unauthorized intrusions and properly dealing with a ransomware attack; (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiffs' and Class Members' Private Information; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiffs and Class Members prompt and accurate notice of the Data Breach.

M. Plaintiffs' Experiences

Plaintiff Michael Meza

208. Plaintiff Meza was a previous employee of OTP.

209. Plaintiff Meza provided his PII to OTP as part of his employment. In requesting and maintaining his PII for employment purposes, OTP expressly and impliedly promised, and undertook a duty, to act reasonably in its handling of Plaintiff Meza's Private Information. OTP, however, did not take proper care of Plaintiff Meza's Private Information, leading to its exposure to and exfiltration by cybercriminals as a direct result of OTP's inadequate security measures.

210. Plaintiff Meza received a letter dated August 26, 2022 from OTP concerning the Data Breach. The letter stated that an unauthorized party gained access to Plaintiff Meza's personal information from data stored on OTP's systems. The notice stated that the compromised information that was present on the impacted files included Plaintiff Meza's name and Social Security number and driver's license number. The notice further encouraged plaintiff "to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring free credit reports for suspicious activity." OTP provided Plaintiff Meza with access to 12 months of credit monitoring and identity protection services through Equifax. OTP's conduct, which allowed the Data Breach to occur, caused Plaintiff Meza significant injuries and harm in several ways. Plaintiff Meza must immediately devote time, energy, and money to: (1) closely monitor his medical statements, bills, records, and credit and financial accounts; (2) change login and password information on any sensitive account even more frequently than he already does; (3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that he is not being targeted in a social engineering or spear phishing attack; (4) search for suitable identity theft protection and credit monitoring services, and pay to protect himself; and

(5) place either a "fraud alert" on his credit file or a "credit freeze." Plaintiff took these measures at the direction of Defendant who directed Plaintiff to take these measures in the Data Breach Notice in order to mitigate his damages.

211. Once PII or PHI is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff Meza will need to maintain these heightened measures for years, and possibly his entire life.

212. As a result of the Data Breach, Plaintiff Meza has suffered emotional distress from the release of his Private Information, which he believed would be protected from unauthorized access and disclosure, including anxiety and stress about unauthorized parties viewing, selling, and or using his Private Information for the purposes of identity theft and fraud.

213. Plaintiff Meza also suffered actual injury from having his Private Information compromised as a result of the Data Breach, including, but not limited to: (a) damage to and diminution in the value of his confidential personal information—a form of property that Plaintiff Meza entrusted to OTP, which was compromised as a result of the Data Breach it failed to prevent and (b) a violation of his privacy rights as a result of OTP's unauthorized disclosure of his Private Information.

214. Plaintiff Meza has spent approximately 2-3 hours changing his passwords, updating his credit cards, and otherwise trying to protect himself against fraudulent activity as a result of the Data Breach. The time spent dealing with the aftermath of the Data Breach is time Plaintiff Meza otherwise would have spent on other activities, such as work and/or recreation. Plaintiff Meza gave his Private Information to OTP as a condition of his employment, with the expectation that OTP would keep his information secure and inaccessible from unauthorized parties.

215. Plaintiff Meza greatly values his privacy, especially while receiving medical services. He would not have worked for OTP had he known that his employer would negligently fail to adequately protect his Private Information.

216. Plaintiff Meza is also at a continued risk of harm because his information remains in OTP's systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as OTP fails to undertake the necessary and appropriate data security measures to protect the Private Information in its possession.

217. As a result of the Data Breach, Plaintiff Meza anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach and OTP's ineffective data security measures. Some harms may not materialize for years after the Data Breach, rendering OTP's notice letter woefully inadequate to address and prevent the fraud that has occurred and will continue to occur through the misuse of Plaintiff's information.

Plaintiff Michael Meeks

218. Plaintiff Meeks' health insurance provider is Humana, which upon information and belief is a health insurance provider customer of OTP.

219. Plaintiff Meeks provided his Private Information to Humana in order to receive health insurance. OTP provides marketing and/or management services to Humana and received Plaintiff Meeks's personal and health information in connection with providing those services. In requesting and maintaining his PII/PHI for its business purposes, OTP expressly and impliedly promised, and undertook a duty, to act reasonably in its handling of Plaintiff Meeks's Private Information. OTP, however, did not take proper care of Plaintiff Meeks's Private Information, leading to its exposure to and exfiltration by cybercriminals as a direct result of OTP's inadequate security measures.

220. Plaintiff Meeks received a letter dated July 27, 2022 from OTP concerning the Data Breach. The letter stated that an unauthorized party gained access to Plaintiff's personal information from data stored on OTP's systems. The notice stated that the compromised information that was present on the impacted files included Plaintiff's name, member ID, and information that he may have provided during a health assessment. The notice further encouraged Plaintiff Meeks "to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring free credit reports for suspicious activity and detect errors." OTP did not provide Plaintiff Meeks with complementary credit monitoring services as a result of the Data Breach. OTP's conduct, which allowed the Data Breach to occur, caused Plaintiff Meeks significant injuries and harm in several ways. Plaintiff Meeks must immediately devote time, energy, and money to: (1) closely monitor his medical statements, bills, records, and credit and financial accounts; (2) change login and password information on any sensitive account even more frequently than he already does; (3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that he is not being targeted in a social engineering or spear phishing attack; (4) search for suitable identity theft protection and credit monitoring services, and pay to protect himself; and (5) place either a "fraud alert" on his credit file or a "credit freeze." Plaintiff took these measures at the direction of Defendant who directed Plaintiff to take these measures in the Data Breach Notice in order to mitigate his damages.

221. Once Private Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff Meeks will need to maintain these heightened measures for years, and possibly his entire life.

222. As a result of the Data Breach, Plaintiff Meeks has suffered emotional distress from the release of his Private Information, which he believed would be protected from unauthorized access and disclosure, including anxiety and stress about unauthorized parties viewing, selling, and or using his Private Information for the purposes of identity theft and fraud.

223. Plaintiff Meeks also suffered actual injury from having his Private Information compromised as a result of the Data Breach, including, but not limited to: (a) damage to and diminution in the value of his confidential personal information—a form of property that Plaintiff Meeks entrusted to OTP, which was compromised as a result of the Data Breach it failed to prevent and (b) a violation of his privacy rights as a result of OTP's unauthorized disclosure of his Private Information.

224. Moreover, subsequent to the data breach, Plaintiff also experienced actual identity theft and fraud, including unauthorized charges deducted from his payment account by a credit building company for a loan that he did not apply for or approve. He has also received several notifications from banks regarding loan payments for loans that he did not originate. Plaintiff Meeks also experienced an inexplicable drop in his credit score by 99 points following the Data Breach. Plaintiff Meeks has also been informed that his SSN is associated with someone's employment at the Candler County Hospital, despite never having worked for this institution. Plaintiff Meeks has attempted to have this corrected, but has been unsuccessful even after numerous communications, causing him further distress. Plaintiff Meeks has further experienced an increase in spam calls and text messages following the Data Breach. Plaintiff Meeks has spent several hours responding to these incidents of identity theft and fraud as a result of the Data Breach. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Meeks otherwise would have spent on other activities, such as work and/or recreation. Plaintiff Meeks

paid for health insurance with the expectation that insurer and its service providers, like OTP, would keep his information secure and inaccessible from unauthorized parties.

225. Plaintiff Meeks greatly values his privacy, especially while receiving medical services. He would not have obtained insurance from Humana, or paid the amount he did to receive insurance, had he known that his healthcare provider's marketing service provider would negligently fail to adequately protect his PII/PHI.

226. Plaintiff is also at a continued risk of harm because his information remains in OTP's systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as OTP fails to undertake the necessary and appropriate data security measures to protect the PII and PHI in its possession.

227. As a result of the Data Breach, Plaintiff Meeks anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach and OTP's ineffective data security measures. Some harms may not materialize for years after the Data Breach, rendering OTP's notice letter woefully inadequate to address and prevent the fraud that has occurred and will continue to occur through the misuse of Plaintiff's information.

Plaintiff Marcie Strickland

228. Plaintiff Strickland's health insurance provider is CareSource of Georgia ("CareSource"), which upon information and belief is a health insurance provider customer of OTP.

229. Plaintiff Strickland provided her Private Information to CareSource in order to receive health insurance. OTP provides marketing and/or management services to CareSource and received Plaintiff Stickland's personal and health information in connection with providing those services. In requesting and maintaining her Private Information for its business purposes, OTP expressly and impliedly promised, and undertook a duty, to act reasonably in its handling of

Plaintiff Stickland's Private Information. OTP, however, did not take proper care of Plaintiff Strickland's Private Information, leading to its exposure to and exfiltration by cybercriminals as a direct result of OTP's inadequate security measures.

230. Plaintiff Strickland received a letter in or around July 2022 from OTP concerning the Data Breach. The letter stated that an unauthorized party gained access to Plaintiff Strickland's personal information from data stored on OTP's systems. The notice stated that the compromised information that was present on the impacted files included Plaintiff Strickland's name, date of birth, address, health conditions, allergy information, member identification number, and medical plan information. OTP did not provide Plaintiff Strickland with complementary credit monitoring services as a result of the Data Breach. OTP's conduct, which allowed the Data Breach to occur, caused Plaintiff Strickland significant injuries and harm in several ways. Plaintiff Strickland must immediately devote time, energy, and money to: (1) closely monitor her medical statements, bills, records, and credit and financial accounts; (2) change login and password information on any sensitive account even more frequently than she already does; (3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that she is not being targeted in a social engineering or spear phishing attack; (4) search for suitable identity theft protection and credit monitoring services, and pay to protect herself; and (5) place either a "fraud alert" on her credit file or a "credit freeze." Plaintiff took these measures at the direction of Defendant who directed Plaintiff to take these measures in the Data Breach Notice in order to mitigate her damages.

231. Once PII or PHI is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff Strickland will need to maintain these heightened measures for years, and possibly her entire life.

232. As a result of the Data Breach, Plaintiff Strickland has suffered emotional distress from the release of her Private Information, which she believed would be protected from unauthorized access and disclosure, including anxiety and stress about unauthorized parties viewing, selling, and or using her Private Information for the purposes of identity theft and fraud.

233. Plaintiff Strickland also suffered actual injury from having her Private Information compromised as a result of the Data Breach, including, but not limited to: (a) damage to and diminution in the value of her confidential personal information—a form of property that Plaintiff Strickland entrusted to OTP, which was compromised as a result of the Data Breach it failed to prevent and (b) a violation of her privacy rights as a result of OTP's unauthorized disclosure of her PHI.

234. Moreover, subsequent to the data breach, Plaintiff also experienced actual identity theft and fraud, including dozens of unauthorized credit inquiries that were not initiated by her, and which have impacted her ability to secure a loan to purchase a home. Plaintiff Strickland further has been receiving increased spam calls, which led her to have to change her phone number. Plaintiff Strickland has spent several hours responding to these incidents of identity theft and fraud and having to change her telephone number as a result of the Data Breach. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Strickland otherwise would have spent on other activities, such as work and/or recreation. Plaintiff paid for health insurance with the expectation that CareSource and its service providers, like OTP, would keep her information secure and inaccessible from unauthorized parties.

235. Plaintiff Strickland greatly values her privacy, especially while receiving medical services. She would not have obtained insurance from CareSource, or paid the amount she did to

receive insurance, had she known that her healthcare provider's marketing service provider would negligently fail to adequately protect her Private Information.

236. Plaintiff Strickland is also at a continued risk of harm because her information remains in OTP's systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as OTP fails to undertake the necessary and appropriate data security measures to protect the Private Information in its possession.

237. As a result of the Data Breach, Plaintiff Strickland anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach and OTP's ineffective data security measures. Some harms may not materialize for years after the Data Breach, rendering OTP's notice letter woefully inadequate to address and prevent the fraud that has occurred and will continue to occur through the misuse of Plaintiff Strickland's information.

Plaintiff Richard Dusterhoft

238. Plaintiff Dusterhoft is a member of Humana through Medicare, which upon information and belief is a health insurance provider customer of OTP.

239. Plaintiff Dusterhoft provided his PII and PHI to Humana in order to receive health insurance. OTP provides marketing and/or management services to Humana and received Plaintiff Dusterhoft's personal and health information in connection with providing those services. In requesting and maintaining his Private Information for its business purposes, OTP expressly and impliedly promised, and undertook a duty, to act reasonably in its handling of Plaintiff Dusterhoft's PII/PHI. OTP, however, did not take proper care of Plaintiff Dusterhoft's PII/PHI, leading to its exposure to and exfiltration by cybercriminals as a direct result of OTP's inadequate security measures.

240. Plaintiff Dusterhoft received a letter dated July 27, 2022 from OTP concerning the Data Breach. The letter stated that an unauthorized party gained access to Plaintiff Dusterhoft's personal information from data stored on OTP's systems. The notice stated that the compromised information that was present on the impacted files included Plaintiff Dusterhoft's name, member ID, and information he may have provided during a health assessment. The notice further encouraged plaintiff "to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring free credit reports for suspicious activity and to detect errors." OTP did not provide Plaintiff Dusterhoft with complementary credit monitoring services as a result of the Data Breach. OTP's conduct, which allowed the Data Breach to occur, caused Plaintiff Dusterhoft significant injuries and harm in several ways. Plaintiff Dusthoft must immediately devote time, energy, and money to: (1) closely monitor his medical statements, bills, records, and credit and financial accounts; (2) change login and password information on any sensitive account even more frequently than he already does; (3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that he is not being targeted in a social engineering or spear phishing attack; (4) search for suitable identity theft protection and credit monitoring services, and pay to protect himself; and (5) place either a "fraud alert" on his credit file or a "credit freeze." Plaintiff Dusterhoft took these measures at the direction of Defendant who directed Plaintiff to take these measures in the Data Breach Notice in order to mitigate his damages.

241. Once PII or PHI is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff Dusterhoft will need to maintain these heightened measures for years, and possibly his entire life.

242. As a result of the Data Breach, Plaintiff Dusterhoft has suffered emotional distress from the release of his Private Information, which he believed would be protected from unauthorized access and disclosure, including anxiety and stress about unauthorized parties viewing, selling, and or using his Private Information for the purposes of identity theft and fraud.

243. Plaintiff Dusterhoft also suffered actual injury from having his PII and PHI compromised as a result of the Data Breach, including, but not limited to: (a) damage to and diminution in the value of his confidential personal information—a form of property that Plaintiff Dusterhoft entrusted to OTP, which was compromised as a result of the Data Breach it failed to prevent and (b) a violation of his privacy rights as a result of OTP's unauthorized disclosure of his PHI.

244. Plaintiff has also received an increase in spam calls following the Data Breach. Plaintiff paid for health insurance with the expectation that Humana and its service providers, like OTP, would keep his information secure and inaccessible from unauthorized parties.

245. Plaintiff Dusterhoft greatly values his privacy, especially while receiving medical services. He would not have obtained insurance from Humana, or paid the amount he did to receive insurance, had he known that his healthcare provider's marketing service provider would negligently fail to adequately protect his Private Information.

246. Plaintiff is also at a continued risk of harm because his information remains in OTP's systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as OTP fails to undertake the necessary and appropriate data security measures to protect the PII and PHI in its possession.

247. As a result of the Data Breach, Plaintiff Dusterhoft anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by

the Data Breach and OTP's ineffective data security measures. Some harms may not materialize for years after the Data Breach, rendering OTP's notice letter woefully inadequate to address and prevent the fraud that has occurred and will continue to occur through the misuse of Plaintiff's information.

Plaintiff Robin Guertin

248. Plaintiff Guertin's health insurance provider is Humana, which upon information and belief is a health insurance provider customer of OTP.

249. Plaintiff Guertin provided her Private Information to Humana in order to receive health insurance. OTP provides marketing and/or management services to Humana and received Plaintiff Guertin's personal and health information in connection with providing those services. In requesting and maintaining her Private Information for its business purposes, OTP expressly and impliedly promised, and undertook a duty, to act reasonably in its handling of Plaintiff Guertin's Private Information. OTP, however, did not take proper care of Plaintiff Guertin's Private Information, leading to its exposure to and exfiltration by cybercriminals as a direct result of OTP's inadequate security measures.

250. Plaintiff Guertin received a letter dated July 27, 2022 from OTP concerning the Data Breach. The letter stated that an unauthorized party gained access to Plaintiff Guertin's personal information from data stored on OTP's systems. The notice stated that the compromised information that was present on the impacted files included Plaintiff Guertin's name, member ID and information Plaintiff Guertin provided during a health assessment. The notice further encouraged plaintiff "to remain vigilant against incidents of identity theft and fraud, to review account statements and explanation of benefits forms, and monitoring free credit reports for suspicious activity, and detect errors." OTP did not provide Plaintiff Guertin with complementary

credit monitoring services as a result of the Data Breach. OTP's conduct, which allowed the Data Breach to occur, caused Plaintiff Guertin significant injuries and harm in several ways. Plaintiff Guertin must immediately devote time, energy, and money to: (1) closely monitor her medical statements, bills, records, and credit and financial accounts; (2) change login and password information on any sensitive account even more frequently than she already does; (3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that she is not being targeted in a social engineering or spear phishing attack; (4) search for suitable identity theft protection and credit monitoring services, and pay to protect herself; and (5) place either a "fraud alert" on her credit file or a "credit freeze." Plaintiff took these measures at the direction of Defendant who directed Plaintiff to take these measures in the Data Breach Notice in order to mitigate her damages.

251. Once Private Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff Guertin will need to maintain these heightened measures for years, and possibly her entire life.

252. As a result of the Data Breach, Plaintiff Guertin has suffered emotional distress from the release of her Private Information, which she believed would be protected from unauthorized access and disclosure, including anxiety and stress about unauthorized parties viewing, selling, and or using her Private Information for the purposes of identity theft and fraud.

253. Plaintiff Guertin also suffered actual injury from having her Private Information compromised as a result of the Data Breach, including, but not limited to: (a) damage to and diminution in the value of her confidential personal information—a form of property that Plaintiff Guertin entrusted to OTP, which was compromised as a result of the Data Breach it failed to

prevent and (b) a violation of her privacy rights as a result of OTP's unauthorized disclosure of her Private Information.

254. Moreover, subsequent to the data breach, Plaintiff Guertin suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII and PHI being placed in the hands of unauthorized third parties. Plaintiff Guertin has spent time proactively responding to the threat of identity theft and fraud as a result of the Data Breach by carefully reviewing her accounts for fraudulent activity. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Guertin otherwise would have spent on other activities, such as work and/or recreation. Plaintiff paid for health insurance with the expectation that Humana and its service providers, like OTP, would keep her information secure and inaccessible from unauthorized parties.

255. Plaintiff Guertin greatly values her privacy, especially while receiving medical services. She would not have obtained health insurance from Humana, or paid the amount she did to receive health insurance, had she known that her healthcare provider's marketing service provider would negligently fail to adequately protect her Private Information.

256. Plaintiff is also at a continued risk of harm because her information remains in OTP's systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as OTP fails to undertake the necessary and appropriate data security measures to protect the PII and PHI in its possession.

257. As a result of the Data Breach, Plaintiff Guertin anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach and OTP's ineffective data security measures. Some harms may not materialize for years

after the Data Breach, rendering OTP's notice letter woefully inadequate to address and prevent the fraud that has occurred and will continue to occur through the misuse of Plaintiff's information.

Plaintiff Shira Haid

258. Plaintiff Haid's health insurance provider at the time of the Data Breach was Common Ground Healthcare Cooperative ("Common Ground"), which upon information and belief is a health insurance provider customer of OTP.

259. Plaintiff Haid provided her Private Information to Common Ground in order to receive health insurance. OTP provides marketing and/or management services to Common Ground and received Plaintiff Haid's personal and health information in connection with providing those services. In requesting and maintaining her Private Information for its business purposes, OTP expressly and impliedly promised, and undertook a duty, to act reasonably in its handling of Plaintiff Haid's Private Information. OTP, however, did not take proper care of Plaintiff Haid's Private Information, leading to its exposure to and exfiltration by cybercriminals as a direct result of OTP's inadequate security measures.

260. Plaintiff Haid received a letter dated August 2, 2022 from OTP concerning the Data Breach. The letter stated that an unauthorized party gained access to Plaintiff's personal information from data stored on OTP's systems. The notice stated that the compromised information that was present on the impacted files included Plaintiff's name, address, date of birth, Member ID Number, Social Security number, description and date of services received, and diagnosis codes. The notice further encouraged plaintiff "to remain vigilant against incidents of identity theft and fraud, to review account statements and explanation of benefits forms, and monitoring free credit reports for suspicious activity, and detect errors." OTP did not provide Plaintiff Haid with complementary credit monitoring services as a result of the Data Breach. OTP's

conduct, which allowed the Data Breach to occur, caused Plaintiff Haid significant injuries and harm in several ways. Plaintiff Haid must immediately devote time, energy, and money to: (1) closely monitor her medical statements, bills, records, and credit and financial accounts; (2) change login and password information on any sensitive account even more frequently than she already does; (3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that she is not being targeted in a social engineering or spear phishing attack; (4) search for suitable identity theft protection and credit monitoring services, and pay to protect herself; and (5) place either a "fraud alert" on her credit file or a "credit freeze." Plaintiff took these measures at the direction of Defendant who directed Plaintiff to take these measures in the Data Breach Notice in order to mitigate her damages.

261. Once Private Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff Haid will need to maintain these heightened measures for years, and possibly his/her entire life.

262. As a result of the Data Breach, Plaintiff Haid has suffered emotional distress from the release of her PII and PHI, which she believed would be protected from unauthorized access and disclosure, including anxiety and stress about unauthorized parties viewing, selling, and or using her PII and PHI for the purposes of identity theft and fraud.

263. Plaintiff Haid also suffered actual injury from having her PII and PHI compromised as a result of the Data Breach, including, but not limited to: (a) damage to and diminution in the value of her confidential personal information—a form of property that Plaintiff Haid entrusted to OTP, which was compromised as a result of the Data Breach it failed to prevent and (b) a violation of her privacy rights as a result of OTP's unauthorized disclosure of her PHI.

264. Moreover, subsequent to the data breach, Plaintiff also experienced actual identity theft and fraud, including the fraudulent transfer of over $10,000 from her bank. Plaintiff Haid has spent approximately 12 hours responding to these incidents of identity theft and fraud as a result of the Data Breach. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Haid otherwise would have spent on other activities, such as work and/or recreation. Plaintiff paid for health insurance with the expectation that Common Ground and its service providers, like OTP, would keep her information secure and inaccessible from unauthorized parties.

265. Plaintiff Haid greatly values her privacy, especially while receiving medical services. She would not have obtained health insurance from Common Ground, or paid the amount she did to receive health insurance, had she known that her healthcare provider's marketing service provider would negligently fail to adequately protect her Private Information.

266. Plaintiff is also at a continued risk of harm because her information remains in OTP's systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as OTP fails to undertake the necessary and appropriate data security measures to protect the Private Information in its possession.

267. As a result of the Data Breach, Plaintiff Haid anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach and OTP's ineffective data security measures. Some harms may not materialize for years after the Data Breach, rendering OTP's notice letter woefully inadequate to address and prevent the fraud that has occurred and will continue to occur through the misuse of Plaintiff's information.

Plaintiff Aria Nardi

268. Plaintiff Nardi's health insurance providers at the time of the Data Breach were Common Ground Healthcare Cooperative ("Common Ground") and Anthem Incorporated ("Anthem"), which upon information and belief are health insurance provider customers of OTP.

269. Plaintiff Nardi provided her Private Information to Common Ground and Anthem in order to receive health insurance. OTP provides marketing and/or management services to Common Ground and Anthem and received Plaintiff Nardi's personal and health information in connection with providing those services. In requesting and maintaining her Private Information for its business purposes, OTP expressly and impliedly promised, and undertook a duty, to act reasonably in its handling of Plaintiff Nardi's Private Information. OTP, however, did not take proper care of Plaintiff Nardi's PII/PHI, leading to its exposure to and exfiltration by cybercriminals as a direct result of OTP's inadequate security measures.

270. Plaintiff Nardi received a letter dated August 2, 2022 from OTP concerning the Data Breach. The letter stated that an unauthorized party gained access to Plaintiff's personal information from data stored on OTP's systems. The notice stated that the compromised information that was present on the impacted files included Plaintiff's name, address, date of birth, Member ID, Social Security number, description and date of services received, and diagnosis codes. The notice further encouraged plaintiff "to remain vigilant against incidents of identity theft and fraud, to review account statements and explanation of benefits forms, and monitoring free credit reports for suspicious activity, and detect errors." OTP did not provide Plaintiff Nardi with complementary credit monitoring services as a result of the Data Breach. OTP's conduct, which allowed the Data Breach to occur, caused Plaintiff Nardi significant injuries and harm in several ways. Plaintiff Nardi must immediately devote time, energy, and money to: (1) closely monitor

her medical statements, bills, records, and credit and financial accounts; (2) change login and password information on any sensitive account even more frequently than she already does; (3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that she is not being targeted in a social engineering or spear phishing attack; (4) search for suitable identity theft protection and credit monitoring services, and pay to protect herself; and (5) place either a "fraud alert" on her credit file or a "credit freeze." Plaintiff took these measures at the direction of Defendant who directed Plaintiff to take these measures in the Data Breach Notice in order to mitigate her damages.

271. Once Private Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff Nardi will need to maintain these heightened measures for years, and possibly his/her entire life.

272. As a result of the Data Breach, Plaintiff Nardi has suffered emotional distress from the release of her Private Information, which she believed would be protected from unauthorized access and disclosure, including anxiety and stress about unauthorized parties viewing, selling, and or using her Private Information for the purposes of identity theft and fraud.

273. Plaintiff Nardi also suffered actual injury from having her Private Information compromised as a result of the Data Breach, including, but not limited to: (a) damage to and diminution in the value of her confidential personal information—a form of property that Plaintiff Nardi entrusted to OTP, which was compromised as a result of the Data Breach it failed to prevent and (b) a violation of her privacy rights as a result of OTP's unauthorized disclosure of her Private Information.

274. Plaintiff Nardi has spent approximately 1.5 hours proactively ensuring her financial security in response to the Data Breach by freezing her credit score. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Nardi otherwise would have spent on other activities, such as work and/or recreation. Plaintiff paid for health insurance with the expectation that Common Ground and Anthem and its service providers, like OTP, would keep her information secure and inaccessible from unauthorized parties.

275. Plaintiff Nardi greatly values her privacy, especially while receiving medical services. She would not have obtained health insurance from Common Ground and Anthem, or paid the amount she did to receive health insurance, had she known that her healthcare provider's marketing service provider would negligently fail to adequately protect her Private Information.

276. Plaintiff is also at a continued risk of harm because her information remains in OTP's systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as OTP fails to undertake the necessary and appropriate data security measures to protect the Private Information in its possession.

277. As a result of the Data Breach, Plaintiff Nardi anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach and OTP's ineffective data security measures. Some harms may not materialize for years after the Data Breach, rendering OTP's notice letter woefully inadequate to address and prevent the fraud that has occurred and will continue to occur through the misuse of Plaintiff Nardi's information.

Plaintiff Sheila Crosby

278. Plaintiff Crosby is a former employee of OTP.

279. Plaintiff Crosby provided her Private Information to OTP in order to secure employment. In requesting and maintaining her Private Information for its business purposes, OTP

expressly and impliedly promised, and undertook a duty, to act reasonably in its handling of Plaintiff Crosby's Private Information. OTP, however, did not take proper care of Plaintiff Crosby's Private Information, leading to its exposure to and exfiltration by cybercriminals as a direct result of OTP's inadequate security measures.

280. Plaintiff Crosby received a letter dated August 26, 2022 from OTP concerning the Data Breach. The letter stated that an unauthorized party gained access to Plaintiff's personal information from data stored on OTP's systems. The notice stated that the compromised information that was present on the impacted files included Plaintiff's name, Social Security number, and financial information. The notice further encouraged plaintiff "to remain vigilant against incidents of identity theft and fraud, to review account statements and explanation of benefits forms, and monitoring free credit reports for suspicious activity, and detect errors." OTP provided Plaintiff Crosby with complementary credit monitoring services for 12 months as a result of the Data Breach. OTP's conduct, which allowed the Data Breach to occur, caused Plaintiff Crosby significant injuries and harm in several ways. Plaintiff Crosby must immediately devote time, energy, and money to: (1) closely monitor her medical statements, bills, records, and credit and financial accounts; (2) change login and password information on any sensitive account even more frequently than she already does; (3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that she is not being targeted in a social engineering or spear phishing attack; (4) search for suitable identity theft protection and credit monitoring services, and pay to protect herself; and (5) place either a "fraud alert" on her credit file or a "credit freeze." Plaintiff took these measures at the direction of Defendant who directed Plaintiff to take these measures in the Data Breach Notice in order to mitigate her damages.

281. Once Private Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff Crosby will need to maintain these heightened measures for years, and possibly his/her entire life.

282. As a result of the Data Breach, Plaintiff Crosby has suffered emotional distress from the release of her Private Information, which she believed would be protected from unauthorized access and disclosure, including anxiety and stress about unauthorized parties viewing, selling, and or using her Private Information for the purposes of identity theft and fraud.

283. Plaintiff Crosby also suffered actual injury from having her Private Information compromised as a result of the Data Breach, including, but not limited to: (a) damage to and diminution in the value of her confidential personal information—a form of property that Plaintiff Crosby entrusted to OTP, which was compromised as a result of the Data Breach it failed to prevent and (b) a violation of her privacy rights as a result of OTP's unauthorized disclosure of her Private Information.

284. Moreover, subsequent to the data breach, Plaintiff Crosby also experienced actual identity theft and fraud, including several attempts of unauthorized charges to her bank account. Plaintiff Crosby has spent approximately 3 hours responding to these incidents of identity theft and fraud as a result of the Data Breach. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Crosby otherwise would have spent on other activities, such as work and/or recreation. Plaintiff accepted employment with OTP with the expectation that OTP would keep her information secure and inaccessible from unauthorized parties.

285. Plaintiff Crosby greatly values her privacy. She would not have accepted employment with OTP had she known that OTP would negligently fail to adequately protect her

Private Information. She is now hesitant to provide Private Information to potential employers because of the Data Breach and subsequent injury.

286. Plaintiff is also at a continued risk of harm because her information remains in OTP's systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as OTP fails to undertake the necessary and appropriate data security measures to protect the Private Information in its possession.

287. As a result of the Data Breach, Plaintiff Crosby anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach and OTP's ineffective data security measures. Some harms may not materialize for years after the Data Breach, rendering OTP's notice letter woefully inadequate to address and prevent the fraud that has occurred and will continue to occur through the misuse of Plaintiff Crosby's information.

Plaintiff Jeffrey Neil Young

288. Plaintiff Young receives Medicare services from Martin's Point Health Care ("Martin's Point"). Martin's Point, in turn, is a customer of the Matrix Medical Network ("Matrix"), which, upon information and belief, is a healthcare provider customer of OTP. Therefore, Plaintiff Young's Private Information was provided to OTP through Martin's Point and Matrix.

289. Plaintiff Young provided his Private Information to Martin's Point and Matrix in order to receive medical care, and in home healthcare visits. OTP provides marketing and/or management services to Matrix and Martin's Point and received Plaintiff Young's personal and health information in connection with providing those services. In requesting and maintaining his Private Information for its business purposes, OTP expressly and impliedly promised, and

undertook a duty, to act reasonably in its handling of Plaintiff Young's Private Information. OTP, however, did not take proper care of Plaintiff Young's Private Information, leading to its exposure to and exfiltration by cybercriminals as a direct result of OTP's inadequate security measures.

290. Plaintiff Young received a letter dated July 28, 2022 from Martin's Point concerning the Data Breach. The letter stated that Martin's Point had recently been contacted by Matrix, a vendor that contracts with Martin's Point, whose own vendor, OTP, was the target of a ransomware attack. The letter explained that OTP had been hired by Matrix to provide printing and mailing services. The notice stated that the compromised information that was present on the impacted files included home health and wellness visit reports prepared by Matrix and sent to OTP for mailing to treating physicians. The letters contained home health visit information including diagnoses, medication, and preventative and chronic care recommendations.

291. While Martin's Point offered Plaintiff Young free identity theft protection services through IDX, OTP did not provide Plaintiff Young with complementary credit monitoring services or identity theft protection as a result of the Data Breach. OTP's conduct, which allowed the Data Breach to occur, caused Plaintiff Young significant injuries and harm in several ways. Plaintiff Young must immediately devote time, energy, and money to: (1) closely monitor his medical statements, bills, records, and credit and financial accounts; (2) change login and password information on any sensitive account even more frequently than he already does; (3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that he is not being targeted in a social engineering or spear phishing attack; (4) search for suitable identity theft protection and credit monitoring services, and pay to protect himself; and (5) place either a "fraud alert" on his/her credit file or a "credit freeze."

292. Once PII or PHI is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff Young will need to maintain these heightened measures for years, and possibly his/her entire life.

293. As a result of the Data Breach, Plaintiff Young has suffered emotional distress and anxiety from the release of his Private Information, which he believed would be protected from unauthorized access and disclosure, including anxiety and stress about unauthorized parties viewing, selling, and or using his Private Information for the purposes of identity theft and fraud.

294. Plaintiff Young also suffered actual injury from having his Private Information compromised as a result of the Data Breach, including, but not limited to: (a) damage to and diminution in the value of his confidential personal information—a form of property that Plaintiff Young entrusted to OTP, which was compromised as a result of the Data Breach it failed to prevent and (b) a violation of his privacy rights as a result of OTP's unauthorized disclosure of his PHI.

295. Moreover, subsequent to the data breach, Plaintiff Young has repeatedly received dangerous spam and phishing texts that have required his diligent review and efforts so that the malware attached to these texts and emails are not triggered, which could negatively impact his legal practice. They have also required his diligent review as he was in the midst of re-mortgaging a home loan and was and is concerned that these emails, texts and phone calls could negatively affect his credit and home loan application. Since the Data Breach, Plaintiff Young had received at least the following emails and texts since being informed of the Data Breach and receiving a Data Breach letter, which were sent to the number and email address provided to OTP: 8/17-voice mail; 8/29-fax; 8/31-fax; 9/15-voice mail; 9/21-fax; 9/22-email; 9/26-email about shared file; 10/5-email; 10/11-false email; 10/19-email; and 11/5-email. These fake voice mails, texts or emails were intended to provoke Plaintiff Young into opening them in order to attach malware or spyware

to his computer system. Each of these was sent to a telephone number or email address that was provided to Martin's Point and Matrix. Plaintiff Young has spent approximately several hours dealing with these spam calls and emails, and also reviewing his credit card bills and credit reports to monitor for fraudulent activity. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Young otherwise would have spent on other activities, such as work and/or recreation. Plaintiff paid for medical services/health insurance with the expectation that Matrix, Martin's Point and its service providers, like OTP, would keep his information secure and inaccessible from unauthorized parties.

296. Plaintiff Young and Class Members have faced and will continue to face a certainly impending and substantial risk of injury as a result of OTP's ineffective data security measures. Some harms may not materialize for years after the Data Breach, rendering any notice letter woefully inadequate to address and prevent the fraud that has occurred and will continue to occur through the misuse of Class Members' information.

297. Plaintiff Young greatly values his privacy, especially while receiving medical services. He would not have obtained medical services from Martin's Point or Matrix, or paid the amount he did to receive medical services, had he known that his healthcare provider's marketing service provider would negligently fail to adequately protect his PII/PHI. He would not have agreed to the home health visit.

298. Plaintiff Young is also at a continued risk of harm because his information remains in OTP's systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as OTP fails to undertake the necessary and appropriate data security measures to protect the Private Information in its possession.

299. As a result of the Data Breach, Plaintiff Young anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach and OTP's ineffective data security measures. Some harms may not materialize for years after the Data Breach, rendering OTP's notice letter woefully inadequate to address and prevent the fraud that has occurred and will continue to occur through the misuse of Plaintiff's information.

CLASS ALLEGATIONS

300. Plaintiffs bring this class action on behalf of themselves and all Members of the following Class of similarly situated persons pursuant to Federal Rule of Civil Procedure 23. The proposed Class is defined as:

> Nationwide Class: All persons in the United States and its territories whose Private Information was compromised in the Data Breach disclosed by OneTouch on or about July 27, 2022, including all who were sent notice of the Data Breach.

301. Alternatively, or in addition to the Nationwide Class, Plaintiffs also seek to represent the following state subclasses defined as:

> Arizona Class: All persons in the State of Arizona whose Private Information was compromised in the Data Breach disclosed by OneTouch on or about July 27, 2022, including all who were sent notice of the Data Breach.
>
> Georgia Class: All persons in the State of Georgia whose Private Information was compromised in the Data Breach disclosed by OneTouch on or about July 27, 2022, including all who were sent notice of the Data Breach.
>
> Maine Class: All persons in the State of Maine whose Private Information was compromised in the Data Breach disclosed by OneTouch on or about July 27, 2022, including all who were sent notice of the Data Breach.
>
> Minnesota Class: All persons in the State of Minnesota whose Private Information was compromised in the Data Breach disclosed by OneTouch on or about July 27, 2022, including all who were sent notice of the Data Breach.
>
> South Carolina Class: All persons in the State of South Carolina whose Private Information was compromised in the Data Breach disclosed by OneTouch on or about July 27, 2022, including all who were sent notice of the Data Breach.

Wisconsin Class: All persons in the State of Wisconsin whose Private Information was compromised in the Data Breach disclosed by OneTouch on or about July 27, 2022, including all who were sent notice of the Data Breach.

302. The Nationwide Class and the State classes are collectively referred to as the "Class." Excluded from the Class is OTP and its affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).

303. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

304. Numerosity: The Members in the Class are so numerous that joinder of all Class Members in a single proceeding would be impracticable. OTP reported that approximately 2,651,396 individuals' information was exposed in the Data Breach.

305. Commonality and Predominance: Common questions of law and fact exist as to all Class Members and predominate over any potential questions affecting only individual Class Members. Such common questions of law or fact include, *inter alia*:

a. Whether OTP had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiffs' and Class Members' Private Information from unauthorized access and disclosure;

b. Whether OTP's actions and its lax data security practices used to protect Plaintiffs' and Class Members' PII and PHI violated the FTC Act, HIPAA, the Wisconsin Constitution, the Wisconsin Right to Privacy statute, Wis. Stat. § 995.50(2) and/or other state laws and/or OTP's other duties discussed herein;

c. Whether OTP failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most

expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiffs and Class Members;

d. Whether Plaintiffs and Class Members suffered injury as a proximate result of OTP's negligent actions or failures to act;

e. Whether OTP failed to exercise reasonable care to secure and safeguard Plaintiffs' and Class Members' Private Information;

f. Whether an implied contract existed between Class Members and OTP providing that OTP would implement and maintain reasonable security measures to protect and secure Class Members' Private Information from unauthorized access and disclosure;

g. Whether injunctive relief is appropriate and, if so, what injunctive relief is necessary to redress the imminent and currently ongoing harm faced by Plaintiffs and Class Members;

h. Whether OTP's actions and inactions alleged herein constitute gross negligence;

i. Whether OTP breached its duties to protect Plaintiffs' and Class Members' Private Information; and

j. Whether Plaintiffs and all other Members of the Class are entitled to damages and the measure of such damages and relief.

306. OTP engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs on behalf of themselves and all other Class Members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

307. Typicality: Plaintiffs' claims are typical of the claims of the Class. Plaintiffs, like all proposed Members of the Class, had their Private Information compromised in the Data Breach. Plaintiffs and Class Members were injured by the same wrongful acts, practices, and omissions

committed by OTP, as described herein. Plaintiffs' claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class Members.

308. Adequacy: Plaintiffs will fairly and adequately protect the interests of the Class Members. Plaintiffs are adequate representatives of the Class in that they have no interests adverse to, or conflict with, the Class they seek to represent. Plaintiffs have retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

309. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiffs and all other Class Members are relatively small compared to the burden and expense that would be required to individually litigate their claims against OTP, so it would be impracticable for Class Members to individually seek redress from OTP's wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Class)

310. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

311. OTP owed a duty to Plaintiffs and all other Class Members to exercise reasonable care in safeguarding and protecting their Private Information in its possession, custody, or control. OTP's duty arose independently from any contract to protect Plaintiffs' and Class Members' Private Information.

312. OTP's duty to use reasonable care arose from several sources, including but not limited to those described below.

313. OTP had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiffs and Class Members were the foreseeable and probable victims of OTP's inadequate security measures. By receiving, maintaining, and handling Plaintiffs' and Class Members' Private Information that is routinely targeted by criminals for unauthorized access, OTP was obligated to act with reasonable care to protect against these foreseeable threats.

314. OTP's duty also arose from OTP's position as a business associate. OTP holds itself out as a trusted business associate of its client-healthcare and -health insurance providers, and thereby assumed a duty to reasonably protect the Private Information it obtains from its clients. Indeed, OTP, which receives, maintains, and handles the private Information from its clients was in a unique and superior position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

315. OTP knew, or should have known, the risks of collecting and storing Plaintiffs' and all other Class Members' Private Information and the importance of maintaining secure systems. OTP knew, or should have known, of the many data breaches that targeted healthcare providers in recent years.

316. Given the nature of OTP's business, the sensitivity and value of the Private Information it maintains, and the resources at its disposal, OTP should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring.

317. OTP breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' Private Information by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Private Information entrusted to it—including Plaintiffs' and Class Members' Private Information.

318. It was reasonably foreseeable to OTP that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' Private Information by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, destruction and/or dissemination of Plaintiffs' and Class Members' Private Information to unauthorized individuals.

319. But for OTP's negligent conduct or breach of the above-described duties owed to Plaintiffs and Class Members, their Private Information would not have been compromised.

320. As a direct and proximate result of OTP's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiffs and all other Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their Private Information; (iii)

breach of the confidentiality of their Private Information; (iv) deprivation of the value of their Private Information, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the imminent and certainly impending increased risks of medical identity theft they face and will continue to face; (vii) actual or attempted fraud; (viii) continued risk of exposure to hackers and thieves of their Personal Information which remains in OPT's possession, custody, and control; and (iv) emotional distress from the unauthorized disclosure of Private Information to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks.

COUNT II
NEGLIGENCE PER SE
(On Behalf of Plaintiffs and the Class)

321. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

322. OTP's duties arise from HIPAA, 42 U.S.C. § 1302(d), *et seq.*

323. OTP is an entity covered under HIPAA, which sets minimum federal standards for privacy and security of PHI.

324. OTP's duties further arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

325. OTP's duties also arise from Section 5 of the FTC Act, 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the

unfair act or practice by a business, such as OTP, of failing to employ reasonable measures to protect and secure Private Information.

326. OTP's duties further arise from the Wisconsin Constitution and the Wisconsin Right to Privacy statute, Wis. Stat. § 995.50(2).

327. OTP violated HIPAA Privacy and Security Rules and Section 5 of the FTC Act, as well as state law, by failing to use reasonable measures to protect Plaintiff's and all other Class Members' Private Information and not complying with applicable industry standards. OTP's conduct was particularly unreasonable given the nature and amount of Private Information it obtains and stores, and the foreseeable consequences of a data breach involving Private Information including, specifically, the substantial damages that would result to Plaintiff and the other Class Members.

328. OTP's violations of HIPAA Privacy and Security Rules and Section 5 of the FTC Act, as well as state law, constitutes negligence per se.

329. Plaintiffs and Class Members are within the class of persons that HIPAA Privacy and Security Rules and Section 5 of the FTC Act, as well as state law, were intended to protect.

330. The harm occurring as a result of the Data Breach is the type of harm HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to guard against.

331. It was reasonably foreseeable to OTP that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' Private Information by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiffs' and Class Members' Private Information to unauthorized individuals.

332. The injury and harm that Plaintiffs and the other Class Members suffered was the direct and proximate result of OTP's violations of HIPAA Privacy and Security Rules and Section 5 of the FTC Act, as well as state law. Plaintiffs and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their Private Information; (iii) breach of the confidentiality of their Private Information; (iv) deprivation of the value of their Private Information, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the certainly impending increased risk of medical identity theft they face and will continue to face; (vi) actual or attempted fraud; (viii) continued risk of exposure to hackers and thieves of their Personal Information which remains in OPT's possession, custody, and control; and (iv) emotional distress from the unauthorized disclosure of personal Information to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks.

COUNT III
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiffs and the Class)

333. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

334. Plaintiffs and Class Members have an interest, both equitable and legal, in the Private Information about them that was conveyed to, collected by, and maintained by OTP and was ultimately accessed or compromised in the Data Breach.

335. As a business associate of its clients, and as a result of its acceptance and storage of its clients' patients and health plan participants Private Information, OTP has a fiduciary duty to Plaintiffs and Class Members. In light of this fiduciary relationship, OTP must act primarily for the benefit of its clients' patients and health plan participants, which includes safeguarding and protecting Plaintiffs' and Class Members' Private Information, even in the absence of direct privity between them.

336. Because of that fiduciary duty, Plaintiffs and Class Members either directly or indirectly gave OTP their Private Information in confidence, believing that OTP would protect that information. Plaintiffs and Class Members would not have provided OTP with this information had they known it would not be adequately protected.

337. OTP has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of their relationship, requiring OTP to exercise the utmost care in safeguarding and protecting Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

338. OTP breached that duty by failing to properly protect the integrity of the system containing Plaintiffs' and Class Members' Private Information, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard the Private Information of Plaintiffs and Class Members it collected.

339. As a direct and proximate result of OTP's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including, but not limited to: (i) a substantial and certainly impending increased risk of identity theft; (ii) the compromise, publication, and theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their Private Information; (iv) lost

opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their Private Information which remains in OTP's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the Private Information compromised as a result of the Data Breach; (vii) actual or attempted fraud; and (viii) emotion distress from the unauthorized disclosure of personal Information to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks.

COUNT IV
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On Behalf of Plaintiffs and the Class)

340. Plaintiffs incorporate by reference the foregoing allegations of fact as if fully set forth herein.

341. Defendant entered into written contracts, including HIPAA Business Associate Agreements, with its clients to perform services that include, but are not limited to, providing care strategies, consulting, analytics, and other services. Upon information and belief, these contracts are virtually identical between and among MCG Health and its medical provider customers around the country whose patients were affected by the Data Breach.

342. In exchange, Defendant agreed, in part, to implement adequate security measures to safeguard the Private Information of Plaintiffs and the Class and to timely and adequately notify them of the Data Breach.

343. These contracts were made expressly for the benefit of Plaintiffs and the Class, as Plaintiffs and Class Members were the intended third-party beneficiaries of the contracts entered into between Defendant and its clients. Defendant knew that if it were to breach these contracts

with its clients, the clients' patients or plan members—Plaintiffs and Class Members—would be harmed.

344. Defendant breached the contracts it entered into with its clients by, among other things, failing to (i) use reasonable data security measures, (ii) implement adequate protocols and employee training sufficient to protect Plaintiffs' Private Information from unauthorized disclosure to third parties, and (iii) promptly and adequately notify Plaintiffs and Class Members of the Data Breach.

345. Plaintiffs and the Class were harmed by Defendant's breach of its contracts with its clients, as such breach is alleged herein, and are entitled to the losses and damages they have sustained as a direct and proximate result thereof.

346. Plaintiffs and Class Members are also entitled to their costs and attorney's fees incurred in this action.

COUNT V
VIOLATIONS OF THE RIGHT TO PRIVACY ACT Wis. Stat. § 995.50(2)
(On Behalf of Plaintiffs and the Class)

347. Plaintiffs and the Class Members incorporate the above allegations as if fully set forth herein.

348. Wisconsin has codified the traditional common law torts of invasion of privacy and intrusion upon seclusion through Wis. Stat. § 995.50(2).

349. OTP violated the Wisconsin Right to Privacy statute by publicizing private details and facts in a place that a reasonable person would consider private, not generally known to the public, not publicly available, without consent and not of legitimate public concern about Plaintiffs and Class Members by disclosing and exposing Plaintiffs' and Class Members' PII and PHI to

enough people that it is reasonably likely those facts will become known to the public at large, including without limitation on the dark web and elsewhere.

350. The disclosure of Plaintiffs' and Class Members' PII and PHI is harmful and highly offensive to a reasonable person of ordinary sensibilities.

351. OTP should appreciate that the cyber-criminals who stole the PII and PHI would further sell and disclose the PII and PHI and that the original disclosure is devastating to the Plaintiffs and the Class Members even though it may have originally only been made to one person or a limited number of cyber-criminals.

352. Under Wisconsin's Right to Privacy statute, the tort of public disclosure of private facts is recognized in Wisconsin. Plaintiffs' and the Class Members' private PII and PHI was publicly disclosed by OTP in the Data Breach with reckless disregard for the reasonable offensiveness of the disclosure. Such disclosure is highly offensive and would be to any person of ordinary sensibilities. OTP knew and knows that Plaintiffs' and Class Members' PII and PHI is not a matter of legitimate public concern.

353. The Wisconsin Right to Privacy statute provides that any person whose privacy is unreasonably invaded is entities to the following relief: (a) Equitable relief to prevent and restrain such invasion, excluding prior restraint against constitutionally protected communication privately and through the public media; (b) Compensatory damages based either on plaintiff's loss or defendant's unjust enrichment; and (c) A reasonable amount for attorney fees." Wis. Stat. § 995.50(2)(1)(a)-(c).

354. As a direct and proximate result of OTP's conduct, Plaintiff and Class Members privacy have been unreasonably invaded and are entitled to equitable relief to prevent and restrain ongoing or future invasions of privacy, compensatory damages based on the harm Plaintiffs and

Class Members' suffered, or alternatively compensatory damages based on OTP's being unjustly enriched by its conduct.

COUNT VI
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Class)

355. Plaintiffs incorporate by reference all allegations of the preceding factual allegations as though fully set forth herein.

356. OTP required Plaintiffs and Class Members to provide, or authorize the transfer of, their Private Information in order for OTP to provide services. In exchange, OTP entered into implied contracts with Plaintiffs and Class Members in which OTP agreed to comply with its statutory and common law duties to protect Plaintiff's and Class Members' Private Information and to timely notify them in the event of a data breach.

357. Plaintiffs and Class Members would not have provided their Private Information to OTP had they known that OTP would not safeguard their Private Information, as promised, or provide timely notice of a data breach.

358. Plaintiffs and Class Members fully performed their obligations under their implied contracts with OTP.

359. OTP breached the implied contracts by failing to safeguard Plaintiffs' and Class Members' Private Information and by failing to provide them with timely and accurate notice of the Data Breach.

360. The losses and damages Plaintiffs and Class Members sustained (as described above) were the direct and proximate result of OTP's breach of its implied contracts with Plaintiffs and Class Members.

COUNT VII
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class)

361. Plaintiffs realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

362. Plaintiffs and Class Members have an interest, both equitable and legal, in the Private Information about them that was conveyed to, collected by, and maintained by OTP and was ultimately accessed or compromised in the Data Breach.

363. Plaintiffs and Class Members conferred a monetary benefit upon OTP in the form of monies paid for healthcare services or other services. OTP's business model would not exist save for the need to ensure the security of Plaintiffs' and Class Members' Private Information in order to provide print, marketing execution, and supply chain management services to client-healthcare and -health insurance providers.

364. The relationship between OTP and Plaintiffs and Class Members is not attenuated, as Plaintiffs and Class Members had a reasonable expectation that the security of their Private Information would be maintained when they provided their Private Information to OTP's client-healthcare and -health insurance providers.

365. OTP accepted or had knowledge of the benefits conferred upon it by Plaintiffs and Class Members. Upon information and belief, this financial benefit was, in part, conferred, when OTP was paid by clients to use Plaintiffs' Private Information to provide print, marketing execution, and supply chain management services to OTP's client-healthcare and -health insurance providers. OTP also benefitted from the receipt of Plaintiffs' and Class Members' Private Information.

366. OTP also understood and appreciated that the Private Information pertaining to Plaintiffs and Class Members was private and confidential and its value depended upon OTP maintaining the privacy and confidentiality of that Private Information.

367. But for OTP's willingness to commit to properly and safely collect, maintain and security Private Information, the Private Information would not have been transferred to and entrusted to OTP. Further, if OTP had disclosed that its security measures were inadequate, OTP would not have gained the trust of its client-healthcare and -health insurance providers.

368. As a result of OTP's wrongful conduct, Plaintiffs and Class Members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiffs and Class Members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

369. OTP's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the collection, maintenance, and inadequate security of Plaintiffs and Class Members Private Information, while at the same time failing to securely maintain that information from unauthorized access and compromise.

370. OTP should not be permitted to retain the money belonging to Plaintiffs and Class Members. It would be unjust, inequitable, and unconscionable to retain the benefits it received and is still receiving from Plaintiffs and Class Members because OTP failed to adequately implement the data privacy and security procedures for itself that Plaintiffs and Class Members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

371. The benefit conferred upon, received, and enjoyed by OTP was not conferred officiously or gratuitously, and it would be inequitable and unjust for OTP to retain the benefit.

372. OTP should be compelled to provide for the benefit of Plaintiffs and Class Members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

COUNT VIII
WISCONSIN CONFIDENTIALITY OF HEALTH RECORDS LAW, WIS. STAT. §146.81, *et seq*.
(On Behalf of Plaintiffs and the Class)

373. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

374. Wisconsin law regarding Confidentiality of Patient Health Care Records, WIS. STAT. §§146.81, *et seq*., states that:

> All patient health care records shall remain confidential. Patient health care records may be released only to the persons designated in this section or to other persons with the informed consent of the patient or of a person authorized by the patient."
>
> WIS. STAT. §146.82(1).

375. OTP disclosed the private and protected medical information of Plaintiffs and Class members to unauthorized third parties without their knowledge, consent, or authorization.

376. Plaintiffs and Class Members provided their Private Information to "health care provider[s]" as defined by WIS. STAT. § 146.81(1).

377. Plaintiffs and Class Members are "patients," as defined by WIS. STAT. § 146.81(3), of OTP's client-healthcare providers.

378. The stolen Private Information belonging to Plaintiffs and Class Members are "health care records" under WIS. STAT. § 146.81(4).

379. OTP is a "covered entity" for purposes of WIS. STAT. § 146.82 and had a duty not to re-disclose any healthcare records in its possession regarding Plaintiffs and members of the Class. WIS. STAT. § 146.82.

380. OTP re-disclosed healthcare care records pertaining to Plaintiffs and Class Members without their consent and for no other reason permitted by either WIS. STAT. § 146.82(5) or § 610.70, and therefore violated WIS. STAT. § 146.82.

381. OTP violated WIS. STAT. §§146.81*, et seq*. through its willful and knowing failure to maintain adequate security measures, which allowed criminals to improperly access and compromise when it compromised, allowed access to, released, and disclosed patient health care records and Private Information without the informed consent or authorization of Plaintiffs and Class Members. OTP did not and does not have express or implied consent to disclose, allow access to, or release the Plaintiffs' and Members' Private Information. To the contrary, OTP expressly undertook a duty and obligation to Plaintiffs and Class Members.

382. Plaintiffs and Class Members were injured and have suffered damages as a result of OTPs illegal disclosure and negligence release of their healthcare records in violation of WIS. STAT. § 146.82.

383. OTP did not disclose to or warn the Plaintiffs and Class Members that their Private Information could be compromised, stolen, released, or disclosed to third parties without their consent as a result of OTP's computer systems and software being outdated, easy to hack, inadequate, and insecure. Plaintiffs and Class Members did not know or expect, or have any reason to know or suspect, that OTP's computer systems and software were so outdated, easy to hack, inadequate, and insecure that it would expose their Private Information to unauthorized disclosure. In fact, they were told to the contrary in written statements and representations given to Plaintiffs and Class Members, and on OTP's website, namely that:

> [OTP] maintains commercially reasonable security measures to protect [Private Information] [OTP] collects and store[s] from loss, misuse, destruction, or unauthorized access.[87]

384. WIS. STAT. §146.84(1)(b) states:

> Any person, including the state or any political subdivision of the state, who violates WIS. STAT. § 146.82 or § 146.83 in a manner that is knowing and willful shall be liable to any person injured as a result of the violation for actual damages to that person, exemplary damages of not more than $25,000 and costs and reasonable attorneys' fees.

385. WIS. STAT. §146.84(1)(bm) states:

> Any person, including the state or any political subdivision of the state, who negligently violates WIS. STAT. §146.82 or 146.83 shall be liable to ***any person injured*** as a result of the violation for actual damages to that person, ***exemplary damages*** of not more than $1,000 and costs and reasonable actual attorney fees. WIS. STAT. §146.84(1)(bm). [Emphasis added.]

386. WIS. STAT. §146.84(1)(c) states:

> An individual may bring an action to enjoin any violation of §§146.82 or 146.83 or to compel compliance with §§146.82 or 146.83 and may, in the same action, seek damages as provided in this subsection.

387. Actual damages are not a prerequisite to liability for statutory or exemplary damages under WIS. STAT. §146.81. A simple comparison of other Wisconsin statues (*e.g.*, WIS. STAT. §134.97(3)(a) and (b), "Civil Liability; Disposal And Use" of records containing personal information), makes clear that the Wisconsin Legislature did not include an actual damages requirement in Wis. Stat. §146.84 when it explicitly did so in other privacy statutes. *See* WIS. STAT. §134.97(3)(a) and (b).

388. Similarly, the Wisconsin legislature made it clear that the exemplary damages referred to WIS. STAT. §146.81 are not the same as punitive damages. Here, the plain language of another Wisconsin statue (WIS. STAT. §895.043(2), "Scope" of punitive damages), specifically

[87] *Privacy Policy*, ONETOUCHPOINT, https://1touchpoint.com/privacy-policy (last visited: August 3, 2022).

and unequivocally excludes an award of "exemplary damages" under WIS. STAT. §§146.84(1)(b) and (bm) from the scope of "punitive damages" available under Section 895.043. In short, exemplary damages under WIS. STAT. §146.84(1)(b) and (bm) are not the same as either actual damages, or punitive damages; they are statutory damages available to persons who have been "injured" as a result of a negligent data breach like the one at issue here The plain, common dictionary definition of "injure" is, "**injured**; **injuring** play \'inj-riŋ, 'in-jə-\

transitive verb
1a : to do an injustice to **:** wrong
b : to harm, impair, or tarnish the standing of
- *injured* his reputation
c : to give pain to
- *injure* a person's pride
2a : to inflict bodily hurt on
b : to impair the soundness of
- *injured* her health
c : to inflict material damage or loss on."[88]

389. Plaintiffs and Class Members request that the Court issue declaratory relief declaring OTP's practice of using insecure, outdated, and inadequate email and computer systems and software that are easy to hack for storage and communication of Private Information data between OTP and third parties unlawful. The Plaintiffs and Class Members further request the Court enter an injunction requiring OTP to cease the unlawful practices described herein, and enjoining OTP from disclosing or using Private Information without first adequately securing or encrypting it.

[88] "Injure" Merriam Webster Online Dictionary (2021 ed.); *see also supra* note 5 (relying on Black's Online Law Dictionary (2d ed.) definition, stating an injury is "Any wrong or damage done to another, either in his person, rights, reputation, or property." *Parker v. Griswold*, 17 Conn.288, 42 Am. Dec. 739; *Woodruff v. North Bloomfield Gravel Mining Co*., 18 Fed.753; *Hitch v. Edgecombe County Comm'rs*, 132 N. C. 573, 44 S.E. 30; *Macauley v. Tierney*, 19 R.I. 255, 33 Atl. 1, 37 L.R.A. 455, 61 Am. St. Rep. 770. In the civil law. A delict committed in contempt or outrage of anyone whereby his body, his dignity, or his reputation is maliciously injured. Voet, Com. Ad Pand. 47, t. 10, no. 1.

390. Plaintiffs and Class Members request the Court order OTP to identify, seek, obtain, encrypt, and retain at the conclusion of this action all existing Private Information in their possession or the possession of third parties and provide it to the Plaintiffs and Class Members.

391. Plaintiffs and Class Members request that the Court enter an injunction ordering that OTP:

a. engage a third-party ombudsman as well as internal compliance personnel to monitor, conduct test, and audit OTP's safeguards and procedures on a periodic basis;

b. audit, test, and train its internal personnel regarding any new or modified safeguards and procedures;

c. conduct regular checks and tests on its safeguards and procedures;

d. periodically conduct internal training and education to inform internal personnel how to immediately identify violations when they occur and what to do in response;

e. meaningfully educate its former and current patients about their privacy rights by, without limitation, written statements describing with reasonable specificity the precautionary steps OTP is taking to update its security technology to adequately secure and safeguard patient Private Information; and

f. identify to each Class Member in writing with reasonable specificity the Private Information of each such Class Member that was stolen in the Data Breach, including without limitation as required under WIS. STAT. §134.98(3)(c).

g. Plaintiffs and Class Members request the Court enter an Order pursuant to WIS. STAT. §146.84(1)(bm) awarding minimum statutory exemplary damages of

$1,000 to each Plaintiff and each Class Member whose Private Information was compromised and stolen, as well as attorneys' fees and costs.

COUNT IX

WISCONSIN DECEPTIVE TRADE PRACTICES ACT, WIS. STAT. §§100.18, *et seq.*, (On Behalf of Plaintiffs and the Class)

392. Plaintiffs re-allege and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

393. OTP's conduct violates Wisconsin's Deceptive Trade Practices Act, WIS. STAT. §100.18 (the "WDTPA"),[89] which provides that no,

> "firm, corporation or association,. . .with intent to sell, distribute, increase the consumption of ... any ... merchandise ... directly or indirectly, to the public for sale ... shall make, publish, disseminate, circulate, or place before the public ... in this state, in a ... label ... or in any other way similar or dissimilar to the foregoing, an advertisement, announcement, statement or representation of any kind to the public ... which ... contains any assertion, representation or statement of fact which is untrue, deceptive or misleading."

394. OTP is a "person, firm, corporation or association," as defined by WIS. STAT. § 100.18(1).

395. Plaintiffs and Class Members are members of "the public," as defined by WIS. STAT. § 100.18(1).

396. Plaintiffs and Class Members "suffered pecuniary loss because of a violation" of the WDTPA. WIS. STAT. §100.18(11)(b)(2).

397. OTP deliberately engaged in deceptive and unlawful practices on or around April 28, 2022, when OTP continued to assert, represent, and state on its website that "We maintain commercially reasonable security measures to protect [Private Information] we collect and store

[89] WIS. STAT. §110.18.

from loss, misuse, destruction, or unauthorized access." Specifically, OTP continued to make this claim even though OTP knew its network had been accessed via the Data Breach.

398. OTP further violated the WDTPA by: (a) fraudulently advertising material facts pertaining to its system and data services by representing and advertising that it would maintain security practices and procedures to safeguard its systems and data from cyberattacks like the Data Breaches, to prevent infiltration of the security system so as to safeguard Private Information from unauthorized access; (b) misrepresenting material facts pertaining to its system and data services by representing and advertising that it would maintain security practices and procedures to safeguard its systems and data from cyberattacks like the Data Breaches, so as to safeguard Private Information from unauthorized access; (c) omitting, suppressing, and concealing the material fact of the inadequacy of the security practices and procedures; (d) engaging in deceptive, unfair, and unlawful trade acts or practices by failing to maintain security practices and procedures to safeguard its systems and data from cyberattacks like the Data Breaches, to prevent infiltration of the security system so as to safeguard Private Information from unauthorized access; and (e) engaging in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the Data Breach to enact reasonable security practices to safeguard its systems and data from cyberattacks like the Data Breaches.

399. OTP intended to mislead Plaintiffs and Class Members and induce them to rely on its misrepresentations and omissions, and therefore increase the sales and use of OTP's goods and services.

400. OTP's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and Class members, about the adequacy of

OTP's security measures and ability to protect the confidentiality of consumers' Private Information.

401. OTP's representations and omissions were further material because they were likely to deceive reasonable consumers, including Plaintiffs and Class members, that their Private Information was not exposed and misled Plaintiffs and Class Members into believing they did not need to take actions to secure their Private Information exposed by OTP.

402. OTP knew or should have known that its computer systems and security practices and procedures were inadequate, and that risk of the Data Breaches and theft was high. OTP's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiffs and Class Members.

403. As a direct and proximate result of OTP's deceptive acts or practices, Plaintiffs and Class Members have suffered and will continue to suffer injury, ascertainable loses of money or property, and monetary and non-monetary damages, including from fraud and identity theft, time and expense relating to monitoring their Private Information for fraudulent activity, an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

404. OTP had an ongoing duty to Plaintiffs and Class members to refrain from deceptive acts, practices, plans, and schemes under WIS. STAT § 100.18.

405. The Plaintiffs and the Class Members reasonably relied upon OTP's deceptive and unlawful marketing practices and are entitled to damages, including reasonable attorney fees and costs, punitive damages, and other relief which the court deems proper. WIS. STAT. §§ 100.18(11)(b)(2) and 100.20(5).

COUNT X
MAINE UNFAIR TRADE PRACTICES ACT, 5 Me. Rev. Stat. §§ 205, 213, *et seq.*
(On Behalf of Plaintiff Young and the Maine Subclass)

406. Plaintiff Young restates and realleges all of the foregoing Paragraphs as if fully set forth herein.

407. Plaintiff Young ("Plaintiff" for the purposes of this Count) brings this Count on his own behalf and on behalf of the Maine Subclass.

408. OTP is a "person" as defined by 5 Me. Stat. § 206(2).

409. OTP's conduct as alleged herein related was in the course of "trade and commerce" as defined by 5 Me. Stat. § 206(3).

410. Plaintiff and Maine Subclass members purchased goods and/or services for personal, family, and/or household purposes.

411. OTP engaged in unfair and deceptive trade acts and practices in the conduct of trade or commerce, in violation of 5 Me. Rev. Stat. §207, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Maine Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Maine Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Maine Subclass members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Maine Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;

f. Failing to timely and adequately notify Plaintiff, and Maine Subclass members of the Data Breach;

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Maine Subclass members' Private Information; and

h. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Maine Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

412. OTP's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of OTP's data security and ability to protect the confidentiality of consumers' Private Information.

413. OTP's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiff and the Maine Subclass members, that their Private Information was not exposed and misled Plaintiff and the Maine Subclass members into believing they did not need to take actions to secure their identities.

414. Had OTP disclosed to Plaintiff and Class members that its data systems were not secure and, thus, vulnerable to attack, OTP would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, OTP was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiff, the Class, and the Maine Subclass. OTP accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because OTP held itself out as maintaining a secure platform for

Private Information data, Plaintiff, the Class, and the Maine Subclass members acted reasonably in relying on OTP's misrepresentations and omissions, the truth of which they could not have discovered.

415. As a direct and proximate result of OTP's unfair and deceptive acts and conduct, Plaintiff and Maine Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial and other accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

416. Plaintiff and the Maine Subclass members seek non-monetary relief allowed by law, including damages or restitution, injunctive and other equitable relief, and attorneys' fees and costs.

417. As of the filing of this complaint Plaintiff has sent a demand for relief on behalf of the Maine Subclass pursuant to 5 Me. Rev. Stat. § 213(1-A) and intends to amend this complaint to seek monetary damages pursuant to the pre-suit notice requirement.

COUNT XI
MAINE UNIFORM DECEPTIVE TRADE PRACTICES ACT,
10 Me. Rev. Stat. §§ 1212, *et seq*.
(On Behalf of Plaintiff Young and the Maine Sub-Class)

418. Plaintiff restates and realleges all of the foregoing Paragraphs as if fully set forth herein.

419. Plaintiff Young ("Plaintiff" for the purposes of this Count) brings this Count on his own behalf and on behalf of the Maine Subclass.

420. OTP is a "person" as defined by 10 Me. Rev. Stat. § 1211(5).

421. OTP advertised, offered, or sold goods or services in Maine and engaged in trade or commerce directly or indirectly affecting the people of Maine.

422. OTP engaged in deceptive trade practices in the conduct of its business, in violation of 10 Me. Rev. Stat. §1212, including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

423. OTP's deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Maine Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Maine Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Maine Subclass members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Maine Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;

f. Failing to timely and adequately notify Plaintiff, and Maine Subclass members of the Data Breach;

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Maine Subclass members' Private Information; and

h. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of

> Plaintiff and Maine Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

424. OTP's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of OTP's data security and ability to protect the confidentiality of consumers' Private Information.

425. OTP's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiff and the Maine Subclass members, that their Private Information was not exposed and misled Plaintiff and the Maine Subclass members into believing they did not need to take actions to secure their identities.

426. OTP intended to mislead Plaintiff and Maine Subclass members and induce them to rely on its misrepresentations and omissions.

427. Had OTP disclosed to Plaintiff and Maine Subclass members that its data systems were not secure and, thus, vulnerable to attack, OTP would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, OTP was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiff, and the Maine Subclass. OTP accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because OTP held itself out as maintaining a secure platform for Private Information data, Plaintiff and the Maine Subclass members acted reasonably in relying on OTP's misrepresentations and omissions, the truth of which they could not have discovered.

428. As a direct and proximate result of OTP's deceptive trade practices, Plaintiff and Maine Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity

theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

429. Maine Subclass members are likely to be damaged by OTP's ongoing deceptive trade practices.

430. Plaintiff and the Maine Subclass members seek all monetary and non-monetary relief allowed by law, including damages or restitution, injunctive or other equitable relief, and attorneys' fees and costs.

COUNT XII
ARIZONA CONSUMER FRAUD ACT, Ariz. Rev. Stat. §§ 44-1521, *et seq*.
(On Behalf of Plaintiff Meza and the Arizona Subclass)

431. Plaintiff Michael Meza identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Arizona Subclass, restates and realleges all of the foregoing Paragraphs as if fully set forth herein. This claim is brought individually under the laws of Arizona and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer fraud.

432. OTP is a "person" as defined by Ariz. Rev. Stat. § 44-1521(6).

433. OTP advertised, offered, or sold goods or services in Arizona and engaged in trade or commerce directly or indirectly affecting the people of Arizona.

434. OTP engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts affecting the people of Arizona in connection with the sale and advertisement of "merchandise" (as defined in Arizona Consumer Fraud Act, Ariz. Rev. Stat. § 44-1521(5)) in violation of Ariz. Rev. Stat. § 44-1522(A), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Arizona Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Arizona Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-05, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Arizona Subclass members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Arizona Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-05;

f. Failing to timely and adequately notify Plaintiff, and Arizona Subclass members of the Data Breach;

g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;

h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Arizona Subclass members' Private Information; and

i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Arizona Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-05.

435. OTP's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of OTP's data security and ability to protect the confidentiality of consumers' Private Information.

436. OTP's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiff and the Arizona Subclass members, that their

Private Information was not exposed and misled Plaintiff and the Arizona Subclass members into believing they did not need to take actions to secure their identities.

437. OTP intended to mislead Plaintiff and Arizona Subclass members and induce them to rely on its misrepresentations and omissions.

438. Had OTP disclosed to Plaintiff and Class members that its data systems were not secure and, thus, vulnerable to attack, OTP would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, OTP was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiff, the Class, and the Arizona Subclass. OTP accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because OTP held itself out as maintaining a secure platform for Private Information data, Plaintiff, the Class, and the Arizona Subclass members acted reasonably in relying on OTP's misrepresentations and omissions, the truth of which they could not have discovered.

439. OTP acted intentionally, knowingly, and maliciously to violate Arizona's Consumer Fraud Act, and recklessly disregarded Plaintiff and Arizona Subclass members' rights.

440. As a direct and proximate result of OTP's unfair and deceptive acts and practices, Plaintiff and Arizona Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

441. Plaintiff and Arizona Subclass members seek all monetary and non-monetary relief allowed by law, including compensatory damages; disgorgement; punitive damages; injunctive relief; and reasonable attorneys' fees and costs.

COUNT XIII
GEORGIA SECURITY BREACH NOTIFICATION ACT, O.C.G.A. §§ 10-1-912, *et seq*.
(On Behalf of Plaintiff Meeks and the Georgia Subclass)

442. Plaintiff Michael Meeks ("Plaintiff," for purposes of this Count), individually and on behalf of the Georgia Subclass, restates and realleges all of the foregoing Paragraphs as if fully set forth herein. This claim is brought individually under the laws of Georgia and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding security breach notification.

443. OTP is a business that owns or licenses computerized data that includes "personal information" as defined by O.C.G.A. § 10-1-912(a).

444. Plaintiff and Georgia Subclass members' Private Information includes "personal information" as covered under O.C.G.A. § 10-1-912(a).

445. OTP is required to accurately notify Plaintiff and Georgia Subclass members if it becomes aware of a breach of its data security program that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Georgia Subclass members' Private Information, in the most expedient time possible and without unreasonable delay under O.C.G.A. § 10-1-912(a).

446. Because OTP was aware of a breach of its security system that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Georgia Subclass members' Private Information, OTP had an obligation to disclose the data breach in a timely and accurate fashion as mandated by O.C.G.A. § 10-1-912(a).

447. By failing to disclose the Data Breach in a timely and accurate manner, OTP violated O.C.G.A. § 10-1-912(a).

448. As a direct and proximate result of OTP's violations of O.C.G.A. § 10-1-912(a), Plaintiff and Georgia Subclass members suffered damages, as described above.

449. Plaintiff and Georgia Subclass members seek relief under O.C.G.A. § 10-1-912 including actual damages and injunctive relief.

COUNT XIV
GEORGIA FAIR BUSINESS PRACTICES ACT, O.C.G.A. § 10-1-390, *et seq.*
(On Behalf of Plaintiff Meeks and the Georgia Subclass)

450. Plaintiff Michael Meeks ("Plaintiff," for purposes of this Count), individually and on behalf of the Georgia Subclass, restates and realleges all of the foregoing Paragraphs as if fully set forth herein. This claim is brought individually under the laws of Georgia and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding fair business practices.

451. OTP's conduct described herein constitutes deceptive acts and practices, which were directed at Plaintiff and Georgia Subclass members, and are violations of Georgia Fair Business Practices Act, O.C.G.A. § 10-1-390, et seq. ("FBPA").

452. OTP, Plaintiff, and Class members are "persons" within the meaning of the Georgia Fair Business Practices Act ("GFBPA"), O.C.G.A. § 10-1-399(a).

453. OTP is engaged in, and its acts and omissions affect, trade and commerce under O.C.G.A. § 10-1-392(28). Further, OTP is engaged in "consumer acts or practices," which are defined as "acts or practices intended to encourage consumer transactions" under O.C.G.A. § 10-1-392(7). OTP, in its capacity as a "consumer reporting agency," generates and maintains "consumer reports" and "files" subject to the GFBPA. O.C.G.A. §10-1-392 (9)-(10), (14).

454. OTP's acts, practices, and omissions at issue in this matter were directed to Plaintiff and Georgia Subclass members.

455. At the time of its misrepresentations and omissions, OTP was either aware that it was failing to adequately maintain and secure Private Information, that the Private Information exposed during the Data Breach did include sensitive Private Information, or was aware that it lacked the information and/or knowledge required to make such a representation truthfully. OTP concealed, omitted and failed to disclose this information to Plaintiffs and Class Members.

456. OTP engaged in "[u]nfair or deceptive acts or practices in the conduct of consumer transactions and consumer acts or practices in trade or commerce" in violation of O.C.G.A. § 10-1-393(a). Those acts and practices include those expressly declared unlawful by O.C.G.A. § 10-1-393(b), such as:

a. Representing that goods or services have characteristics that they do not have;
b. Representing that goods or services are of a particular standard, quality, or grade if they are of another; and
c. Advertising goods or services with intent not to sell them as advertised.

457. In addition, OTP engaged in the unfair and deceptive acts and practices described below that, while not expressly declared unlawful by O.C.G.A. § 10-1-393(b), are prohibited by O.C.G.A. § 10-1-393(a).

458. In the course of its business, OTP engaged in unfair acts and practices prohibited by O.C.G.A. § 10-1-393(a), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Class members' Private Information, which was a direct and proximate cause of the Data Breach and its immense scope;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, adequately improve security and privacy measures following previous cybersecurity incidents, and detect and redress the Data

Breach while it was ongoing, which were a direct and proximate cause of the Data Breach and its immense scope; and

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach and its immense scope.

d. In the course of its business, OTP also engaged in deceptive acts and practices prohibited by O.C.G.A. § 10-1-393(a), including:

e. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class members' Private Information, including by implementing and maintaining reasonable security measures;

f. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;

g. Failing to timely and adequately notify the Plaintiff, and Georgia Subclass members of the Data Breach;

h. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;

i. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class members' Private Information; and

j. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security of Plaintiff and Class members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

459. The misrepresentations and omissions described in the preceding paragraph were material and made intentionally and knowingly with the intent that Plaintiff, Class members, and others (such as its customers, regulators, investors, and those who otherwise used data from OTP for business purposes) rely upon them in connection with accessing and storing the extremely sensitive and valuable Private Information of Plaintiff and Class members.

460. OTP's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiff and the Georgia Subclass members, that their Private Information was not exposed and misled Plaintiff and the Georgia Subclass members into believing they did not need to take actions to secure their identities.

461. Prior to the Data Breach, OTP knew of the inadequate security controls and vulnerabilities in its systems and networks containing Plaintiff and the Georgia Subclass members' sensitive and valuable Private Information but failed to remedy the inadequacies to protect this information.

462. OTP's deceptive acts and practices were likely to and did in fact deceive the public at large and reasonable consumers, including Plaintiff and Georgia Subclass members, regarding the security and safety of the Private Information in its care, including the Private Information of Plaintiff and Georgia Subclass members. OTP's deceptive acts and practices also were intended to and did in fact deceive others who relied upon OTP to maintain the security of the Private Information in its care, including its customers, regulators, and others who used data from OTP for business purposes.

463. OTP's representations and omissions were material to Plaintiff and the Georgia Subclass given the extreme sensitivity, value, and importance of the Private Information maintained by OTP; the uncertainty and disruption that would inevitably occur if the marketplace were informed OTP did not adequately protect Private Information; and the obvious adverse consequences to participants in the American economy from a substantial data breach at OTP.

464. OTP knew or should have known that by collecting, selling, and trafficking in Private Information, Plaintiff and, Georgia Subclass members would reasonably rely upon and assume OTP's data systems were secure unless OTP otherwise informed them.

465. Because OTP's primary product was the sale and analysis of highly sensitive Private Information, and because OTP controlled the compilation of and access to such Private Information, Plaintiff and Georgia Subclass members relied upon OTP to advise if its data systems were not secure and, thus, Private Information could be compromised.

466. Plaintiff, Georgia Subclass members, and others who relied upon OTP to maintain adequate data security programs had no effective means on their own to discover the truth. In particular, OTP did not afford Plaintiff and Georgia Subclass members any opportunity to inspect OTP's data security, learn that it was inadequate and non-compliant with legal requirements, or otherwise ascertain the truthfulness of OTP's representations and omissions regarding OTP's ability to protect data and comply with the law.

467. Plaintiffs and Georgia Subclass members, relied to their detriment upon OTP's representations and omissions regarding data security, including OTP's failure to alert customers that its privacy and security protections were inadequate and insecure and thus were vulnerable to attack.

468. Had OTP disclosed to Plaintiff, Georgia Subclass members, and others (such as the Social Good Entities, regulators, and others who used data from OTP for business purposes) that its data systems were not secure and, thus, vulnerable to attack, OTP would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law.

469. Instead, OTP was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiff and the Georgia Subclass. OTP accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public.

470. Accordingly, because OTP held itself out as maintaining a secure platform for Private Information data, Plaintiff and the Georgia Subclass members acted reasonably in relying on OTP's misrepresentations and omissions, the truth of which they could not have discovered.

471. OTP acted intentionally, knowingly, and maliciously to violate the GFBPA, and recklessly disregarded Plaintiff's and Class members' rights.

472. OTP's violations present a continuing risk to Plaintiff and Georgia Subclass members, as well as to the general public.

473. OTP's unlawful acts and practices complained of herein affect the consumer marketplace and the public interest, including the millions of U.S. residents, which include Georgians affected by the Data Breach.

474. But for OTP's violations of the GFBPA described above, the Data Breach would not have occurred.

475. As a direct and proximate result of OTP's violations of the GFBPA, Plaintiff and Georgia Subclass members have suffered injury-in-fact, monetary, and non-monetary damages, including damages from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information, and/or actual damages, as described herein.

476. The GFBPA permits any person who suffers injury or damages as a result of the violation of its provisions to bring an action against the person or persons engaged in such violations. O.C.G.A. § 10-1-399(a).

477. Pursuant to O.C.G.A. § 10-1-399(b), on February 24, 2021, at least 30 days prior to bringing this claim, Plaintiff and the Georgia Subclass provided OTP with a written demand for relief describing the unfair or deceptive act or practice relied upon and the injury suffered by them.

More than 30 days have elapsed since the service of that written demand. No written tender of settlement has been made by OTP.

478. Plaintiff bring this action on behalf of themselves and Georgia Subclass members for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow consumers and the public at large to make informed decisions related to the security of their sensitive Private Information, and to protect the public from OTP's unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and unlawful practices.

479. Plaintiff and Georgia Subclass members are entitled to a judgment against OTP for actual and consequential damages; general, nominal, exemplary, and trebled damages and attorneys' fees pursuant to the GFBPA; costs; and such other further relief as the Court deems just and proper.

COUNT XV
GEORGIA UNIFORM DECEPTIVE TRADE PRACTICES ACT, O.C.G.A. §§ 10-1-370, *et seq*.
(On Behalf of Plaintiff Meeks and the Georgia Subclass)

480. Plaintiff Michael Meeks ("Plaintiff," for purposes of this Count), individually and on behalf of the Georgia Subclass, restates and realleges all of the foregoing Paragraphs as if fully set forth herein. This claim is brought individually under the laws of Georgia and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding deceptive trade practices.

481. OTP, Plaintiff, and Georgia Subclass members are "persons" within the meaning of § 10-1-371(5) of the Georgia Uniform Deceptive Trade Practices Act ("Georgia UDTPA").

482. OTP engaged in deceptive trade practices in the conduct of its business, in violation of O.C.G.A. § 10-1-372(a), including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

483. OTP's deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Georgia Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Georgia Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Georgia Subclass members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Georgia Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;

f. Failing to timely and adequately notify Plaintiff, and Georgia Subclass members of the Data Breach;

g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;

h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Georgia Subclass members' Private Information; and

i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of

Plaintiff and Georgia Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

484. OTP's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of OTP's data security and ability to protect the confidentiality of consumers' Private Information.

485. OTP's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiff and the Georgia Subclass members, that their Private Information was not exposed and misled Plaintiff and the Georgia Subclass members into believing they did not need to take actions to secure their identities.

486. OTP intended to mislead Plaintiff and Georgia Subclass members and induce them to rely on its misrepresentations and omissions.

487. In the course of its business, OTP engaged in activities with a tendency or capacity to deceive.

488. OTP acted intentionally, knowingly, and maliciously to violate Georgia's Uniform Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Georgia Subclass members' rights.

489. Had OTP disclosed to Plaintiff and Georgia Subclass members that its data systems were not secure and, thus, vulnerable to attack, OTP would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, OTP was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiff and the Georgia Subclass. OTP accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because OTP held itself out as maintaining a secure platform for Private Information data, Plaintiff, the Class, and the Georgia Subclass members acted

reasonably in relying on OTP's misrepresentations and omissions, the truth of which they could not have discovered.

490. As a direct and proximate result of OTP's deceptive trade practices, Plaintiff and Georgia Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

491. Plaintiff and Georgia Subclass members seek all relief allowed by law, including injunctive relief, and reasonable attorneys' fees and costs, under O.C.G.A. § 10-1-373.

COUNT XVI
MINNESOTA CONSUMER FRAUD ACT, Minn. Stat. §§ 325F.68, *et seq*. and Minn. Stat. §§ 8.31, *et seq*. (On Behalf of Plaintiff Dusterhoft and the Minnesota Subclass)

492. Plaintiff Richard Dusterhoft ("Plaintiff," for purposes of this Count), individually and on behalf of the Minnesota Subclass, restates and realleges all of the foregoing Paragraphs as if fully set forth herein. This claim is brought individually under the laws of Minnesota and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer fraud.

493. OTP, Plaintiff, and members of the Minnesota Subclass are each a "person" as defined by Minn. Stat. § 325F.68(3).

494. OTP's goods, services, commodities, and intangibles are "merchandise" as defined by Minn. Stat. § 325F.68(2).

495. OTP engaged in "sales" as defined by Minn. Stat. § 325F.68(4).

496. OTP, as the guardian and gatekeeper of Plaintiff's and Minnesota Subclass members' Private Information, had special knowledge of material facts to which Plaintiff and Minnesota Subclass members did not.

497. These material facts included, inter alia, that OTP's systems and networks were vulnerable to unauthorized access and exfiltration, and therefore, Plaintiff and Minnesota Subclass members' Private Information was vulnerable to being exposed, exfiltrated, and misused as a result of a Data Breach.

498. Further, OTP had special knowledge once the Data Breach occurred of material facts to which Plaintiff and Minnesota Subclass members did not. This special knowledge was due to OTP's discovery of the cyberattack and subsequent forensic investigation into what Private Information was exposed, that Plaintiff and Minnesota Subclass members did not have access too.

499. These material facts included, inter alia, that Plaintiff's and Subclass members' Private Information was accessed and infiltrated.

500. Despite holding such special knowledge, OTP failed to disclose these material facts to Plaintiff and Minnesota Subclass members to enable them to decide whether to entrust Private Information to OTP or for Plaintiff and Minnesota Subclass members to take appropriate actions to secure their identities.

501. OTP further engaged in fraud, false pretense, false promise, misrepresentation, misleading statements, and deceptive practices in connection with the sale of merchandise, in violation of Minn. Stat. § 325F.69(1), including:

502. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Minnesota Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;

a. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

b. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Minnesota Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach;

c. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Minnesota Subclass members' Private Information, including by implementing and maintaining reasonable security measures;

d. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Minnesota Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;

e. Failing to timely and adequately notify Plaintiff and Minnesota Subclass members of the Data Breach;

f. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Minnesota Subclass members' Private Information; and

h. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Minnesota Subclass members' Private Information, including duties imposed the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

503. OTP's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of OTP's data security and ability to protect the confidentiality of consumers' Private Information.

504. OTP's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiff and the Minnesota Subclass members, that their

Private Information was not exposed and misled Plaintiff and the Minnesota Subclass members into believing they did not need to take actions to secure their identities.

505. OTP intended to mislead Plaintiff and Minnesota Subclass members and induce them to rely on its misrepresentations and omissions.

506. OTP's fraudulent, misleading, and deceptive practices affected the public interest, including millions of Minnesotans affected by the Data Breach.

507. As a direct and proximate result of OTP's fraudulent, misleading, and deceptive practices, Plaintiff and Minnesota Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

508. Plaintiff and Minnesota Subclass members seek injunctive relief requiring OTP to adequately protect Plaintiff and Minnesota Subclass members' Private Information from future cyber-attacks, and to require that OTP provide Plaintiff and Minnesota Subclass members with sufficient resources to safeguard their identities related to the risks arising from the Data Breach at issue.

509. Such remedies would provide a public benefit aimed at altering OTP's conduct, protecting Plaintiff and Minnesota Subclass members' Private Information, and providing resources for continued, future efforts of safeguarding their identities related to the risks arising from the Data Breach at issue.

510. Plaintiff and Minnesota Subclass members further seek all monetary and non-monetary relief allowed by law, including damages; injunctive or other equitable relief; and attorneys' fees, disbursements, and costs.

COUNT XVII
MINNESOTA UNIFORM DECEPTIVE TRADE PRACTICES ACT,
Minn. Stat. §§ 325D.43, *et seq*.
(On Behalf of Plaintiff Dusterhoft and the Minnesota Subclass)

511. Plaintiff Richard Dusterhoft ("Plaintiff," for purposes of this Count), individually and on behalf of the Minnesota Subclass, restates and realleges all of the foregoing Paragraphs as if fully set forth herein. This claim is brought individually under the laws of Minnesota and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding deceptive trade practices.

512. By engaging in deceptive trade practices in the course of its business and vocation, directly or indirectly affecting the people of Minnesota, OTP violated Minn. Stat. § 325D.44, including the following provisions:

a. Representing that its goods and services had characteristics, uses, and benefits that they did not have, in violation of Minn. Stat. § 325D.44(1)(5);

b. Representing that goods and services are of a particular standard or quality when they are of another, in violation of Minn. Stat. § 325D.44(1)(7);

c. Advertising goods and services with intent not to sell them as advertised, in violation of Minn. Stat. § 325D.44(1)(9); and

d. Engaging in other conduct which similarly creates a likelihood of confusion or misunderstanding, in violation of Minn. Stat. § 325D.44(1)(13).

e. OTP's deceptive practices include:

f. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Minnesota Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;

g. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

h. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Minnesota Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach;

i. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Minnesota Subclass members' Private Information, including by implementing and maintaining reasonable security measures;

j. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Minnesota Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;

k. Failing to timely and adequately notify Plaintiff and Minnesota Subclass members of the Data Breach;

l. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;

m. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Minnesota Subclass members' Private Information; and

n. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Minnesota Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

513. OTP's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of OTP's data security and ability to protect the confidentiality of consumers' Private Information.

514. OTP's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiff and the Minnesota Subclass members, that their Private Information was not exposed and misled Plaintiff and the Minnesota Subclass members into believing they did not need to take actions to secure their identities.

515. OTP intended to mislead Plaintiff and Minnesota Subclass members and induce them to rely on its misrepresentations and omissions.

516. Had OTP disclosed to Plaintiff and Class members that its data systems were not secure and, thus, vulnerable to attack, OTP would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, OTP was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiff, the Class, and the Minnesota Subclass. OTP accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because OTP held itself out as maintaining a secure platform for Private Information data, Plaintiff, the Class, and the Minnesota Subclass members acted reasonably in relying on OTP's misrepresentations and omissions, the truth of which they could not have discovered.

517. OTP acted intentionally, knowingly, and maliciously to violate Minnesota's Uniform Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Minnesota Subclass members' rights.

518. Plaintiff and Minnesota Subclass members are likely to be damaged in the future given that OTP still maintains their Private Information, continues to adequately safeguard and protect this information from unauthorized access in the future, and therefore, has created a likelihood that such information may be exposed during a future Data Breach.

519. As a direct and proximate result of OTP's deceptive trade practices, Plaintiff and Minnesota Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

520. Plaintiff and Minnesota Subclass members seek injunctive relief requiring OTP to adequately protect Plaintiff and Minnesota Subclass members' Private Information from future cyber-attacks, and to require that OTP provide Plaintiff and Minnesota Subclass members with sufficient resources to safeguard their identities related to the risks arising from the Data Breach at issue.

521. Such remedies would provide a public benefit aimed at altering OTP's conduct, protecting Plaintiff and Minnesota Subclass members' Private Information, and providing resources for continued, future efforts of safeguarding their identities related to the risks arising from the Data Breach at issue.

522. Plaintiff and Minnesota Subclass members further seek all monetary and non-monetary relief allowed by law, including damages; injunctive or other equitable relief; and attorneys' fees, disbursements, and costs.

COUNT XVIII
MINNESOTA HEALTH RECORDS ACT, Minn. Stat. § 144.291, *et seq.*

523. Plaintiff Richard Dusterhoft ("Plaintiff," for purposes of this Count), individually and on behalf of the Minnesota PHI Subclass, restates and realleges all of the foregoing Paragraphs as if fully set forth herein. This claim is brought individually under the laws of Minnesota and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding health records.

524. At all relevant times, Plaintiff was a "patient" of a healthcare organization (to which he provided her PHI) which is a "provider", as those terms are construed under the Minnesota Health Records Act. See Minn. Stat. § 144.291, Subd. 2(g) and (i).

525. At all times relevant to this action, OTP stored "health care records" of the Plaintiff and other Minnesota PHI Subclass members as those terms are construed under the Minnesota

Health Records Act in connection with the operation of OTP's business. See Minn. Stat. § 144.291, Subd. 2(c).

526. Absent an applicable exception under the statute or other law, the Minnesota Health Records Act makes it unlawful for someone, such as OTP, who receives records from a provider to release a patient's health care records to a third party without the patient's signed and dated consent. See Minn. Stat. § 144.293, Subd. 2 and 5.

527. None of the exceptions to the requirement to obtain a patient's consent to release health care records are applicable to OTP's release of health care records at issue here. See Minn. Stat. § 144.293, Subd. 5.

528. Plaintiff and other Minnesota PHI Subclass members did not provide consent to release their health care records to third parties.

529. OTP negligently or intentionally disclosed and released Plaintiff's and the Minnesota PHI Subclass members' health care records inasmuch as it did not implement adequate security protocols to prevent unauthorized access to health care records, maintain an adequate electronic security system to prevent data breaches, or employ industry standard and commercially viable measures to mitigate the risks of any data the risks of any data breach or otherwise comply with HIPAA data security requirements.

530. As a direct and proximate result of OTP's negligent or intentional acts, it disclosed and released Plaintiff's health care records to third parties without the Plaintiff's consent and caused injury to the Plaintiff and the Minnesota PHI Subclass.

531. OTP's unauthorized disclosure of medical records has caused injury to the Plaintiff and the Minnesota PHI Subclass.

532. Accordingly, Plaintiff, individually and on behalf of members of the Minnesota PHI Subclass, seek compensatory damages plus costs and attorney fees. See Minn. Stat. § 144.298.

COUNT XIX
SOUTH CAROLINA DATA BREACH SECURITY ACT, S.C. Code Ann. §§ 39-1-90, *et seq*.
(On Behalf of Plaintiff Guertin and the South Carolina Subclass)

533. Plaintiff Robin Guertin ("Plaintiff," for purposes of this Count), individually and on behalf of the South Carolina Subclass, restates and realleges all of the foregoing Paragraphs as if fully set forth herein. This claim is brought individually under the laws of South Carolina and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding data breach security.

534. OTP is a business that owns or licenses computerized data or other data that includes personal identifying information as defined by S.C. Code Ann. § 39-1-90(A). OTP is contractually entitled to this information through its contracts with its healthcare and health insurance provider clients.

535. Plaintiff and South Carolina Subclass members' Private Information includes personal identifying information as covered under S.C. Code Ann. § 39-1-90(D)(3).

536. OTP is required to adequately notify Plaintiff and South Carolina Subclass members following discovery or notification of a breach of its data security program if Private Information that was not rendered unusable through encryption, redaction, or other methods was, or was reasonably believed to have been, acquired by an unauthorized person, creating a material risk of harm, in the most expedient time possible and without unreasonable delay under S.C. Code Ann. § 39-1-90(A).

537. Because OTP discovered a breach of its data security program in which Private Information that was not rendered unusable through encryption, redaction, or other methods, was,

or was reasonably believed to have been, acquired by an unauthorized person, creating a material risk of harm, OTP had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by S.C. Code Ann. § 39-1-90(A).

538. By failing to disclose the Data Breach in a timely and accurate manner, OTP violated S.C. Code Ann. § 39-1-90(A).

539. As a direct and proximate result of OTP's violations of S.C. Code Ann. § 39-1-90(A), Plaintiff and South Carolina Subclass members suffered damages, as described above.

540. Plaintiffs and South Carolina Subclass members seek relief under S.C. Code Ann. § 39-1-90(G), including actual damages and injunctive relief.

COUNT XX
DECLARATORY AND INJUNCTIVE RELIEF
(On Behalf of Plaintiffs and the Class)

541. Plaintiffs and the Class Members incorporate the above allegations as if fully set forth herein.

542. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

543. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and Class Members' Private Information and whether OTP is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their Private Information. Plaintiffs allege that OTP's data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise

of their Private Information and remain at imminent risk that further compromises of their Private Information still in OTP's possession, custody, and control will occur in the future.

544. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. A declaration that OTP owes a legal duty to secure Private Information obtained from its client health care and health insurance providers and to timely notify Plaintiffs and Class Members of such a data breach under the common law, Section 5 of the FTC Act, HIPAA, and state law;

b. A declaration that OTP breached and continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII and PHI;

c. A declaration that OTP's acts and omissions as alleged herein violate applicable state law; and

d. A declaration that OTP's practice of using insecure, outdated, and inadequate email and computer systems and software that are easy to hack for storage and communication of PII and PHI data between OTP and third parties is unlawful.

545. This Court should also issue corresponding prospective relief requiring OTP to:

a. cease the unlawful practices described herein, and enjoining OTP from disclosing or using PII or PHI without first adequately securing or encrypting it;

b. seek, obtain, encrypt, and retain at the conclusion of this action all existing PII and PHI in their possession or the possession of third parties and provide it to Plaintiffs and the Class Members;

c. engage a third-party ombudsman as well as internal compliance personnel to monitor, conduct, test, and audit OTP's safeguards and procedures on a periodic basis;

d. audit, test, and train its internal personnel regarding any new or modified safeguards and procedures;

e. conduct regular checks and tests on its safeguards and procedures;

f. periodically conduct internal training and education to inform internal personnel how to immediately identify violations when they occur and what to do in response;

g. meaningfully educate its former and current employees about their privacy rights by, without limitation, written statements describing with reasonable specificity the precautionary steps OTP is taking to update its security technology to adequately secure and safeguard employee PII; and

h. identify to each Class Member in writing with reasonable specificity the PII and personal information of each such Class Member that was stolen in the Data Breach.

546. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at OTP. The risk of another such breach is real, immediate, and substantial. If another breach at OTP occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

547. The hardship to Plaintiffs and Class Members if an injunction does not issue exceeds the hardship to OTP if an injunction is issued. Plaintiffs will likely be subjected to

substantial identity theft and other damage. On the other hand, the cost to OTP of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and OTP has a pre-existing legal obligation to employ such measures.

548. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at OTP, thus eliminating the additional injuries that would result to Plaintiffs, Class Members, and consumers whose Private Information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all other Members of the Class, respectfully request that the Court enter judgment in her favor and against OTP as follows:

A. Certifying the Class as requested herein, designating Plaintiffs as Class representative, and appointing Plaintiffs' counsel as Class Counsel;

B. Awarding Plaintiffs and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiffs and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiffs, on behalf of themselves and the Class, seeks appropriate injunctive relief designed to prevent OTP from experiencing another data breach by adopting and implementing best data security practices to safeguard Private Information and to provide or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;

D. Awarding Plaintiffs and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiffs and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiffs and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury of all claims in this Consolidated Class Action Complaint so triable.

Dated: November 14, 2022

Respectfully submitted,

/s/ Gary M. Klinger

Gary M. Klinger
MILBERG, COLEMAN, PHILLIPS, GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (866) 252-0878
gklinger@milberg.com

Gary F. Lynch
LYNCH CARPENTER, LLP
1133 Penn Avenue, Floor 5
Pittsburgh, PA 15222
Phone: (412) 322-9243
GaryLynchLaw.com

Interim Co-Lead Counsel for all Plaintiffs

Benjamin F. Johns
CHIMICLES SCHWARTZ KRINER & DONALDSON-SMITH LLP
One Haverford Centre
361 Lancaster Avenue
Haverford, PA 19041
Phone: (610) 642-8500
bfj@chimicles.com

Joseph M. Lyon
THE LYON FIRM
2754 Erie Avenue
Cincinnati, OH 45208
Phone: (513) 496.1880

Raina C. Borrelli
TURKE & STRAUSS, LLP
613 Williamson St #201
Madison, WI 53703
Phone: (608) 237-1775
raina@turkestrauss.com

Joseph P. Guglielmo
SCOTT+SCOTT ATTORNEYS AT LAW, LLP
The Helmsley Building
230 Park Avenue, 17th Floor
New York, NY 10169
Phone: (212) 223-6444
jguglielmo@scott-scott.com

William B. Federman
FEDERMAN & SHERWOOD
10205 North Pennsylvania Avenue
Oklahoma City, OK 73120
Phone: (405) -235-1560
wbf@federmanlaw.com

Lynda J. Grant
THE GRANT LAW FIRM, PLLC
521 5th Avenue
New York, NY 10175
Phone: (212) 292-4441
lgrant@grantfirm.com

Plaintiffs' Steering Committee

*admission to be sought

Counsel for Plaintiffs and the Proposed Class